Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006215

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-196531
Filing date: 02 July 2004 (02.07.2004)

Date of receipt at the International Bureau: 09 June 2005 (09.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/006215

日本国特許庁
JAPAN PATENT OFFICE

24.03.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　７月　２日
出願番号 Application Number:	特願２００４－１９６５３１
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－１９６５３１
出願人 Applicant(s):	松下電器産業株式会社

２００５年　５月２６日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０４５６４

【書類名】　特許願
【整理番号】　2048160232
【提出日】　平成16年 7月 2日
【あて先】　特許庁長官殿
【国際特許分類】　G09L 1/00
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　野仲　真佐男
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　布田　裕一
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　中野　稔久
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　横田　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　宮崎　雅也
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　山本　雅哉
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　村瀬　薫
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1

【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
不正コンテンツを検知する不正コンテンツ検知システムであって、
　前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
　前記配布センタは、
　前記コンテンツを入力する入力部と、
　認証情報生成情報を保持する認証情報生成情報格納部と、
　前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
　前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、
　一以上の前記検証データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、
　前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
　前記実行装置は、
　前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、
　前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
　前記認証情報を検証するための検証情報を保持する検証情報格納部と、
　前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記一以上の第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、
　前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
　を備えることを特徴とする不正コンテンツ検知システム。
【請求項２】
不正コンテンツを検知する不正コンテンツ検知システムであって、
　前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、
　前記配布センタは、
　前記コンテンツを入力する入力部と、
　認証情報生成情報を保持する認証情報生成情報格納部と、
　前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
　前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含む

データに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、
一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、
前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
前記実行装置は、
前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、
前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする不正コンテンツ検知システム。
【請求項３】
コンテンツを実行、もしくは再生する実行装置であって、
前記実行装置は、
前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記第一属性値の数に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする実行装置。
【請求項４】
コンテンツを実行、もしくは再生する実行装置であって、
前記実行装置は、
前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、

前記認証情報を検証するための検証情報を保持する検証情報格納部と、
前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、
前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、
を備えることを特徴とする実行装置。
【請求項５】
前記取得部は、可搬媒体からデータを取得すること、
を特徴とする、請求項３または請求項４に記載の実行装置。
【請求項６】
前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、
を特徴とする、請求項３または請求項４に記載の実行装置。
【請求項７】
前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、
を特徴とする、請求項３から請求項６のいずれか１項に記載の実行装置。
【請求項８】
前記実行装置は、さらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、
前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、
を特徴とする、請求項３から請求項７のいずれか１項に記載の実行装置。
【請求項９】
前記実行装置は、さらに、
前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、
前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、
を特徴とする、請求項８に記載の実行装置。
【請求項１０】
前記実行装置は、さらに、
デバイス鍵を保持するデバイス鍵格納部と、
前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、
前記取得部はさらに、前記暗号化鍵束を受信すること、
を特徴とする、請求項８または請求項９に記載の実行装置。
【請求項１１】
前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、
を特徴とする、請求項３から請求項１０のいずれか１項に記載の実行装置。
【請求項１２】

前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること
、
を特徴とする、請求項３から請求項１０のいずれか１項に記載の実行装置。
【請求項１３】
前記検証情報は、デジタル署名方式の検証鍵であること、
を特徴とする、請求項３から請求項１２のいずれか１項に記載の実行装置。
【請求項１４】
前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、
前記取得部はさらに、前記検証情報識別子を受信し、
前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、
を特徴とする、請求項３から請求項１３のいずれか１項に記載の実行装置。
【請求項１５】
前記取得部はさらに、前記検証情報を受信すること、
を特徴とする、請求項３から請求項１４のいずれか１項に記載の実行装置。
【請求項１６】
前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、
前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、
を特徴とする、請求項１４から請求項１５のいずれか１項に記載の実行装置。
【請求項１７】
前記実行装置は、さらに、
前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、前記検証情報格納部に保持する第二取得部を備えること、
を特徴とする、請求項１６に記載の実行装置。
【請求項１８】
前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、
を特徴とする、請求項１７に記載の実行装置。
【請求項１９】
前記第二取得部と前記取得部は等しいこと、
を特徴とする、請求項１７または請求項１８に記載の実行装置。
【請求項２０】
前記コンテンツは、前記実行装置で実行可能なプログラムであり、
前記実行部は、前記プログラムを実行すること、
を特徴とする請求項３から請求項１９のいずれか１項に記載の実行装置。
【請求項２１】
コンテンツを配布する配布センタであって、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含む

データに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、
一以上の前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、
前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
を備えることを特徴とする配布センタ。
【請求項２２】
コンテンツを配布する配布センタであって、
前記配布センタは、
前記コンテンツを入力する入力部と、
認証情報生成情報を保持する認証情報生成情報格納部と、
前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、
前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、
一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、
前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、
を備えることを特徴とする配布センタ。
【請求項２３】
前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、
を特徴とする、請求項２１または請求項２２に記載の配布センタ。
【請求項２４】
前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、
を特徴とする、請求項２１から請求項２３のいずれか１項に記載の配布センタ。
【請求項２５】
前記配布センタはさらに、
コンテンツ鍵を保持するコンテンツ鍵格納部と、
前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、
前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、
を特徴とする、請求項２１から請求項２４のいずれか１項に記載の配布センタ。
【請求項２６】
前記配布センタはさらに
一以上のデバイス鍵を保持する実行装置情報格納部と、
前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、
前記配布部はさらに、前記暗号化鍵束を配布すること、
を特徴とする、請求項２５に記載の配布センタ。
【請求項２７】
前記配布センタはさらに

前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、
前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、
を特徴とする、請求項２５または請求項２６に記載の配布センタ。
【請求項２８】
前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、
を特徴とする、請求項２１から請求項２７のいずれか１項に記載の配布センタ。
【請求項２９】
前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、
を特徴とする、請求項２１から請求項２７のいずれか１項に記載の配布センタ。
【請求項３０】
前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、
を特徴とする、請求項２１から請求項２９のいずれか１項に記載の配布センタ。
【請求項３１】
前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布すること、
を特徴とする、請求項２１から請求項３０のいずれか１項に記載の配布センタ。
【請求項３２】
前記配布センタはさらに、
前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテンツ位置情報生成部を備えること、
を特徴とする、請求項２１から請求項３１のいずれか１項に記載の配布センタ。
【請求項３３】
前記コンテンツ位置情報生成部はさらに
外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、
を特徴とする、請求項３２に記載の配布センタ。
【請求項３４】
前記コンテンツ位置情報生成部はさらに、
ランダムに前記コンテンツ位置情報を生成すること、
を特徴とする、請求項３２に記載の配布センタ。

【書類名】明細書
【発明の名称】不正コンテンツ検知システム
【技術分野】
【０００１】
本発明は不正なコンテンツを検知する技術に関するものである。
【背景技術】
【０００２】
近年、デジタルコンテンツの普及に伴い、著作権を保持する者以外がデジタルコンテンツを不正に販売する、いわゆる違法コンテンツの不正配布が社会問題となってきている。このコンテンツ不正配布の一つのケースとして、映画館等で上映される映画コンテンツを、著作権を保持しない第三者がデジタルビデオカメラ等で盗撮し、その盗撮した動画コンテンツを光ディスクに記録し販売するというものが挙げられる。また別のケースとして、正規に販売されている片面２層ＤＶＤ－ＲＯＭディスク（最大８．５ギガバイト）に記録されているＤＶＤ－ＶＩＤＥＯ形式の映画コンテンツの画質を変換処理して４．７ギガバイト以下に収まるようにして、片面１層ＤＶＤ－Ｒディスク（最大４．７ギガバイト）に記録して販売するものも挙げられる。
【０００３】
上記のようなコンテンツ不正利用を防ぐ方法の従来技術としては、特許文献１に記載されている不正コンテンツ検知システムが知られている。この従来技術は、可搬媒体の中に、コンテンツデータの他に、複数の部分コンテンツデータに対応するハッシュ値と、複数のハッシュ値を結合したデータに対する著作権者のデジタル署名と、を記録しておく。そして、実行装置では、可搬媒体の中のコンテンツを再生する前と、コンテンツを再生している途中に、記録されたコンテンツデータが正規の著作権者によって記録されたものか、デジタル署名及びハッシュ値を用いて検証を行う。そして、検証が失敗したら、コンテンツの再生を停止するものである。こうすることにより、正規の著作権者でない第三者が映画館等において盗撮したコンテンツを可搬媒体に記録して販売したとしても、その可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置はコンテンツを正しく再生しない。これにより、不正なコンテンツの配布防止につながる。
【０００４】
ここでは、従来技術の詳細の一例について図３３を用いて説明する。前提として、正規の著作権者はデジタル署名を作成するための署名生成鍵を有しており、実行装置はその署名生成鍵に対応する署名検証鍵を有しているとする。
【０００５】
初めに、正規の著作権者が、コンテンツデータと、複数の部分コンテンツデータに対応するハッシュ値と、複数のハッシュ値を結合したデータに対するデジタル署名と、を記録した可搬媒体を生成する場合の動作について説明する。まず、デジタルコンテンツをｃ個（ｃは２以上の自然数）のコンテンツブロック（図３３のコンテンツブロック　ＢＬＫ１・・・ＢＬＫｃに対応）に分割する。そして、一方向性関数を用いてコンテンツブロックＢＬＫ１のハッシュ値ＨＡＳＨ１を計算する。コンテンツブロックＢＬＫ２以降も同様にハッシュ値を計算し、それぞれのコンテンツブロックＢＬＫ２、・・・、ＢＬＫｃに対応するハッシュ値ＨＡＳＨ２、・・・、ＨＡＳＨｃを求める。そして、ｃ個のハッシュ値ＨＡＳＨ１、・・・、ＨＡＳＨｃを連結させたものをヘッダ情報ＨＥＡＤとする。その後、正規の著作権者の署名生成鍵を用いて、そのヘッダ情報ＨＥＡＤのデジタル署名を生成し、そのデジタル署名とヘッダ情報とコンテンツを可搬媒体に記録し、実行装置へ提供する。
【０００６】
続いて、実行装置が、提供された可搬媒体内のコンテンツを再生する場合の動作について説明する。まず、署名検証鍵を用いてデジタル署名が正規の著作権者によるヘッダ情報のデジタル署名であるかを検証する。そこで、もし正規のデジタル署名であることが確認されれば、コンテンツの再生を開始する。その後、実行装置はコンテンツを再生しながら

、再生しているコンテンツブロックのハッシュ値を計算し続ける。そして、次のコンテンツブロックに再生位置が移動する際に、計算したハッシュ値がヘッダ情報のハッシュ値と一致するかを確認し、もし一致しなかった場合、コンテンツの再生を停止する。

【０００７】

このような従来技術により、何らかの理由によりコンテンツが盗み出され、そのコンテンツを可搬媒体に記録して販売しようとしても、可搬媒体には正規の著作権者のデジタル署名が記録されていないため、実行装置ではそのコンテンツを再生開始しないか、もしくは、途中で再生が停止する。これにより、不正なコンテンツ流通に対する対策が可能となる。

【特許文献１】米国特許第６４８０９６１号明細書
【特許文献２】特開２００２－２８１０１３号公報
【非特許文献１】「情報セキュリティ」宮地充子・菊池浩明編著　情報処理学会編集
【非特許文献２】「ＴＨＥ　ＡＲＴ　ＯＦ　ＣＯＭＰＵＴＥＲ　ＰＲＯＧＲＡＭＭＩＮＧ　Ｖｏｌ．２　～　ＳＥＭＩＮＵＭＥＲＩＣＡＬ　ＡＬＧＯＲＩＴＨＭＳ」　ＤＯＮＡＬＤ　Ｅ．　ＫＮＵＴＨ　著、ＩＳＢＮ　０－２０１－０３８２２－６

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかしながら、前記従来技術では、実行装置がコンテンツを再生している間、継続してコンテンツブロックのハッシュ値を計算し続けなければならないので、コンテンツ再生中の実行装置の処理負荷が高いという課題を有していた。例えば、一般に、コンテンツは暗号化されて配布されるため、再生する直前にコンテンツを復号化する必要がある。このような場合、コンテンツを復号化すると同時に、復号化したコンテンツのハッシュ値を計算しなければならないという課題があった。

【０００９】

本発明は、前記従来技術の課題を解決するもので、コンテンツ再生中の実行装置の処理負荷を軽減させた不正コンテンツ検知システムを提供することを目的とする。

【課題を解決するための手段】

【００１０】

上記課題を解決するために、請求項１における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選

択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記一以上の第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００１１】

請求項２における発明は、不正コンテンツを検知する不正コンテンツ検知システムであって、前記不正コンテンツ検知システムは、可搬媒体、もしくは記録媒体、もしくは通信ネットワーク、もしくは放送網を介して、前記コンテンツを配布する配布センタと、前記配布センタから受け取った前記コンテンツを実行、もしくは再生する実行装置と、から構成され、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、前記実行装置は、前記コンテンツと、前記付加情報と、前記認証情報と、を取得する取得部と、前記コンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００１２】

請求項３における発明は、コンテンツを実行、もしくは再生する実行装置であって、前記実行装置は、前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記第一属性値の数に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属

性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００１３】

請求項４における発明は、コンテンツを実行、もしくは再生する実行装置であって、前記実行装置は、前記コンテンツと、付加情報と、認証情報と、を取得する取得部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記認証情報を検証するための検証情報を保持する検証情報格納部と、前記コンテンツ位置情報を構成する一以上の前記特定情報の中から全部もしくは一部の一以上の前記特定情報を選択し、選択された前記一以上の特定情報からなる被選択コンテンツ位置情報を生成し、前記コンテンツ及び前記被選択コンテンツ位置情報を基に、前記被選択コンテンツ位置情報に含まれる前記特定情報のそれぞれに対応する前記被選択部分コンテンツを取得し、前記被選択部分コンテンツのそれぞれに対応する第三属性値を生成し、前記属性値比率に基づく個数の前記第一属性値及びそれぞれの前記第三属性値を基に一以上の前記第四属性値を生成し、一以上の前記第四属性値及び前記付加情報に含まれる一以上の前記第二属性値を基に検証対象データを作成し、前記検証対象データ及び予め定められた前記属性値比率及び前記検証情報を基に、前記認証情報を検証する認証情報検証部と、前記認証情報検証部での検証結果が正当な場合にのみ、前記コンテンツを実行開始、もしくは再生開始する実行部と、を備えることを特徴とする。

【００１４】

請求項５における発明は、請求項３または請求項４に記載の実行装置であって、前記取得部は、可搬媒体からデータを取得すること、を特徴とする。

【００１５】

請求項６における発明は、請求項３または請求項４に記載の実行装置であって、前記取得部は、記録媒体、もしくは通信ネットワーク、もしくは放送網からデータを取得すること、を特徴とする。

【００１６】

請求項７における発明は、請求項３から請求項６のいずれか１項に記載の実行装置であって、前記取得部はさらに、外部から前記コンテンツ位置情報を受信し、受信した前記コンテンツ位置情報を前記コンテンツ位置情報格納部に保持すること、を特徴とする。

【００１７】

請求項８における発明は、請求項３から請求項７のいずれか１項に記載の実行装置であって、前記実行装置は、さらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを復号化する部分復号化部と、を備え、前記取得部はさらに、前記コンテンツ鍵を基に前記コンテンツが暗号化された暗号化コンテンツを受信すること、を特徴とする。

【００１８】

請求項９における発明は、請求項８に記載の実行装置であって、前記実行装置は、さらに、前記コンテンツ鍵を基に暗号化された前記コンテンツ位置情報である暗号化コンテンツ位置情報を復号化するコンテンツ位置情報取得部と、を備え、前記取得部はさらに、前記暗号化コンテンツ位置情報を受信すること、を特徴とする。

【００１９】

請求項１０における発明は、請求項８または請求項９に記載の実行装置であって、前記実行装置は、さらに、デバイス鍵を保持するデバイス鍵格納部と、前記デバイス鍵を基に前記コンテンツ鍵が暗号化された暗号化鍵束を復号化するコンテンツ鍵取得部と、を備え、前記取得部はさらに、前記暗号化鍵束を受信すること、を特徴とする。

【００２０】

請求項１１における発明は、請求項３から請求項１０のいずれか１項に記載の実行装置であって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。

【００２１】

請求項１２における発明は、請求項３から請求項１０のいずれかに記載の実行装置であって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。

【００２２】

請求項１３における発明は、請求項３から請求項１２のいずれか１項に記載の実行装置であって、前記検証情報は、デジタル署名方式の検証鍵であること、を特徴とする。

【００２３】

請求項１４における発明は、請求項３から請求項１３のいずれか１項に記載の実行装置であって、前記検証情報格納部は、複数の前記検証情報、及び、複数の前記検証情報に対応付けられた検証情報識別子を保持し、前記取得部はさらに、前記検証情報識別子を受信し、前記検証部は、前記コンテンツ及び前記コンテンツ位置情報を基に、前記代表部分コンテンツを取得し、前記代表部分コンテンツ、及び、前記認証情報、及び、前記検証情報識別子に対応する前記検証情報を基に、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【００２４】

請求項１５における発明は、請求項３から請求項１４のいずれか１項に記載の実行装置であって、前記取得部はさらに、前記検証情報を受信すること、を特徴とする。

【００２５】

請求項１６における発明は、請求項１４または請求項１５に記載の実行装置であって、前記検証情報格納部はさらに、無効化された前記検証情報に関する情報である無効検証情報を保持し、前記検証部はさらに、前記無効検証情報に前記検証情報が含まれていない場合にのみ、前記コンテンツの実行開始、もしくは再生開始を許可するかどうかを決定すること、を特徴とする。

【００２６】

請求項１７における発明は、請求項１６に記載の実行装置であって、前記実行装置は、さらに、前記無効検証情報を、可搬媒体、もしくは、通信路、もしくは、放送網を介して受信し、前記検証情報格納部に保持する第二取得部を備えること、を特徴とする。

【００２７】

請求項１８における発明は、請求項１７に記載の実行装置であって、前記第二取得部は、受信した前記無効検証情報が、前記検証情報格納部に格納されている前記無効検証情報よりも新しい場合にのみ、受信した前記無効検証情報を前記検証情報格納部に保持すること、を特徴とする。

【００２８】

請求項１９における発明は、請求項１７または請求項１８に記載の実行装置であって、前記第二取得部と前記取得部は等しいこと、を特徴とする。

【００２９】

請求項２０における発明は、請求項３から請求項１９のいずれか１項に記載の実行装置であって、前記コンテンツは、前記実行装置で実行可能なプログラムであり、前記実行部は、前記プログラムを実行すること、を特徴とする。

【００３０】

請求項２１における発明は、コンテンツを配布する配布センタであって、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性

値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証対象データ及び前記コンテンツ位置情報に含まれるデータ及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、を備えることを特徴とする。

【００３１】

請求項２２における発明は、コンテンツを配布する配布センタであって、前記配布センタは、前記コンテンツを入力する入力部と、認証情報生成情報を保持する認証情報生成情報格納部と、前記コンテンツの一部分である部分コンテンツに対応する特定情報を一以上含むコンテンツ位置情報を保持するコンテンツ位置情報格納部と、前記コンテンツ及び前記コンテンツ位置情報に含まれる一以上の前記特定情報を基に、対応するそれぞれの部分コンテンツを取得し、一以上の前記部分コンテンツの一部を含むデータに対する第一属性値をそれぞれ生成し、一以上の前記第一属性値を含む第一属性値群を一以上作成し、前記第一属性値群に対する第二属性値をそれぞれ生成し、一以上の前記第二属性値を一以上含む検証対象データを生成する検証対象データ生成部と、一以上の前記検証対象データ及び予め定められている属性値比率及び前記認証情報生成情報を基に、一以上の認証情報を生成する認証情報生成部と、前記コンテンツと、それぞれの前記第一属性値及び一以上の前記検証対象データを含む付加情報と、前記認証情報と、を前記実行装置に配布する配布部と、を備え、を備えることを特徴とする。

【００３２】

請求項２３における発明は、請求項２１または請求項２２に記載の配布センタであって、前記配布部は、可搬媒体、もしくは記録媒体、もしくは通信路、もしくは放送網を用いてデータを配布すること、を特徴とする。

【００３３】

請求項２４における発明は、請求項２１から請求項２３のいずれか１項に記載の配布センタであって、前記配布部はさらに、前記コンテンツ位置情報格納部が保持する前記コンテンツ位置情報を配布すること、を特徴とする。

【００３４】

請求項２５における発明は、請求項２１から請求項２４のいずれか１項に記載の配布センタであって、前記配布センタはさらに、コンテンツ鍵を保持するコンテンツ鍵格納部と、前記コンテンツ鍵を基に、前記コンテンツを暗号化し、暗号化コンテンツを生成する第二暗号化部と、を備え、前記配布部は、前記コンテンツの替わりに前記暗号化コンテンツを配布すること、を特徴とする。

【００３５】

請求項２６における発明は、請求項２５に記載の配布センタであって、前記配布センタはさらに一以上のデバイス鍵を保持する実行装置情報格納部と、前記デバイス鍵のそれぞれを基に、前記コンテンツ鍵を暗号化し、一以上の暗号化コンテンツ鍵を生成し、その一以上の前記暗号化コンテンツ鍵を結合した暗号化鍵束を生成する暗号化鍵束生成部と、を備え、前記配布部はさらに、前記暗号化鍵束を配布すること、を特徴とする。

【００３６】

請求項２７における発明は、請求項２５または請求項２６のいずれか１項に記載の配布センタであって、前記配布センタはさらに前記コンテンツ鍵を基に、前記コンテンツ位置情報を暗号化し、暗号化コンテンツ位置情報を生成する暗号化部を備え、前記配布部はさらに、前記暗号化コンテンツ位置情報を配布すること、を特徴とする。

【００３７】

請求項２８における発明は、請求項２１から請求項２７のいずれか１項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するデジタル署名であること、を特徴とする。

【００３８】
請求項２９における発明は、請求項２１から請求項２７のいずれか１項に記載の配布センタであって、前記認証情報は、前記代表部分コンテンツに対するハッシュ値のデジタル署名であること、を特徴とする。
【００３９】
請求項３０における発明は、請求項２１から請求項２９のいずれか１項に記載の配布センタであって、前記認証情報生成情報は、デジタル署名方式の署名生成鍵であること、を特徴とする。
【００４０】
請求項３１における発明は、請求項２１から請求項３０のいずれか１項に記載の配布センタであって、前記配布部はさらに、無効化された前記検証情報に関する情報である無効検証情報を配布すること、を特徴とする。
【００４１】
請求項３２における発明は、請求項２１から請求項３１のいずれか１項に記載の配布センタであって、前記配布センタはさらに、前記コンテンツ位置情報を生成し、前記コンテンツ位置情報格納部に格納するコンテンツ位置情報生成部を備えること、を特徴とする。
【００４２】
請求項３３における発明は、請求項３２に記載の配布センタであって、前記コンテンツ位置情報生成部はさらに外部からの要求情報を基に、前記コンテンツ位置情報を生成すること、を特徴とする。
【００４３】
請求項３４における発明は、請求項３２に記載の配布センタであって、前記コンテンツ位置情報生成部はさらに、ランダムに前記コンテンツ位置情報を生成すること、を特徴とする。
【発明の効果】
【００４４】
本発明の不正コンテンツ検知システムによれば、コンテンツを実行開始、もしくは再生開始する前にのみ、コンテンツが正規の著作権者により配布されたコンテンツ（正規コンテンツ）なのか、正規の著作権者以外により配布されたコンテンツ（不正コンテンツ）なのかを検証し、コンテンツの実行中、再生中にはその検証を行わないようにした。そうすることにより、不正コンテンツの実行、再生を制限（開始不許可など）することが出来るようになるとともに、従来技術に比べ、コンテンツ実行中、再生中の実行装置の処理負荷を軽減出来るようになった。
【００４５】
また、本発明の不正コンテンツ検知システムでは、さらに、実行装置がコンテンツを実行、再生開始する場合に、暗号化コンテンツの一部分の属性値（ハッシュ値）を検証するようにした。これにより、従来技術のように、暗号化コンテンツを一度復号化して属性値を検証する場合に比べ、処理時間を短縮することが出来た。
【００４６】
また、検証時に、実行装置が同じコンテンツを実行、再生する場合にも、コンテンツの中の毎回異なる一部分の属性値（ハッシュ値）を検証するようにした。これにより、不正者は、次にコンテンツのどの一部分が検証されるのか予測出来ないようになった。
【００４７】
この結果、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを実行、再生する場合でも、ある確率（実行装置が不正な部分コンテンツに入れ替えた部分の属性値を検証する場合）で実行、再生の制限（再生不許可など）が出来るようになる。つまり、ある正規コンテンツの一部を不正な部分コンテンツに入れ替えたような不正コンテンツを、毎回必ず実行、再生をさせることは出来なく出来る。このことにより、コンテンツの中の全部もしくは一部分を、不正なコンテンツに差し替えられるような攻撃を防ぐことが出来、抑止力となる。

【００４８】
これは、コンテンツデータとともに、そのコンテンツデータ全体に対する属性値（ハッシュ値）１つと、その属性値（ハッシュ値）に対するデジタル署名と、を記録した可搬媒体を配布する自明な方式に比べても優位性を持つ。何故なら、自明な方式の場合コンテンツデータ全体に対する属性値（ハッシュ値）を計算しなくてはならないため、コンテンツの実行、再生開始前の処理に時間がかかっていた。しかし、本発明の不正コンテンツ検知システムによれば、コンテンツの実行、再生開始前には、毎回異なるコンテンツの一部分の属性値（ハッシュ値）だけを計算すれば良いので、自明な方式に比べ、処理時間を短縮することが出来る。
【発明を実施するための最良の形態】
【００４９】
以下本発明の実施の形態について、図面を参照しながら説明する。
【００５０】
（実施の形態１）
図１は、本発明の実施の形態１における不正コンテンツ検知システムの構成図である。図１において、配布センタ１０は外部からコンテンツＣＮＴを受け取り、後述する実行装置１２がコンテンツＣＮＴを実行するために必要となる情報を後述する可搬媒体１１に記録するものであり、可搬媒体１１は実行装置１２がコンテンツＣＮＴを実行するために必要となる情報が記録されているものであり、複数の実行装置１２は可搬媒体１１に記録されている情報を用いて、コンテンツＣＮＴを実行するものである。
【００５１】
不正コンテンツ検知システム１は、配布センタ１０（正規のコンテンツ提供者、著作権者、正規の光ディスクプレス業者など）が、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）等の可搬媒体１１の配布手段によって、暗号化されたコンテンツＣＮＴである暗号化コンテンツＥＮＣＣＮＴと、暗号化コンテンツＥＮＣＣＮＴを基に生成されるヘッダ情報ＨＥＡＤと、ヘッダ情報ＨＥＡＤに含まれる第二ハッシュテーブルＨＡＳＨＴＢＬ２の正当性を示す情報である認証情報ＡＵＴＨを、各実行装置１２へ配布する。各実行装置１２は、暗号化コンテンツＥＮＣＣＮＴを基にヘッダ情報ＨＥＡＤの中の一部の情報を入れ替えて入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を作成し、認証情報ＡＵＴＨが配布センタ１０による入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２の正規の認証情報であることを確認し、コンテンツＣＮＴを実行開始する。
【００５２】
以上が、本実施の形態の概要である。以下に、本発明の不正コンテンツ検知システムの一実施の形態である不正コンテンツ検知システム１の詳細について説明を行う。
【００５３】
＜不正コンテンツ検知システム１の構成＞
不正コンテンツ検知システム１は、図１に示すように、配布センタ１０と、可搬媒体１１と、ｓ個の実行装置１２（ｓは１以上の自然数）から構成される。
【００５４】
以下に、これらの構成要素について、詳細に説明する。まず、配布センタ１０の構成と動作について述べ、続いて可搬媒体１１の構成について述べ、最後に実行装置１２の構成と動作について述べる。
【００５５】
＜配布センタ１０の構成＞
配布センタ１０は、図２に示すように、入力部１０１、コンテンツ鍵生成部１０２、実行装置情報格納部１０３、暗号化鍵束生成部１０４、暗号化部１０５、ヘッダ情報生成部１０６、認証情報生成情報格納部１０７、認証情報生成部１０８、配布部１０９から構成される。
【００５６】
（１）入力部１０１

入力部１０１は、外部からコンテンツＣＮＴを入力出来るものである。入力部１０１は、例えば、可搬媒体であるＤＶＤ－ＲＯＭ等からコンテンツＣＮＴを読み取る機能を有する。外部から入力されるコンテンツＣＮＴは、実行装置１２で実行可能なフォーマット形式であって、例えば、ＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ）２フォーマット形式による動画データやＭＰ３フォーマットによる音声データなどである。外部からコンテンツＣＮＴが入力された場合、コンテンツ鍵生成要求ＲＥＱをコンテンツ鍵生成部１０２へ出力し、コンテンツＣＮＴを暗号化部１０５へ出力する。

【００５７】

（２）コンテンツ鍵生成部１０２

コンテンツ鍵生成部１０２は、入力部１０１からコンテンツ鍵生成要求ＲＥＱが入力された場合、コンテンツ鍵ＣＫを生成する。コンテンツ鍵ＣＫを生成する方法としては、例えば、乱数を用いて１２８ビット鍵データをランダムに生成する方法などがあり、これはコンテンツ鍵生成部１０２が乱数生成手段を有していることにより実現出来る。乱数を生成する方法については、非特許文献２が詳しい。そして、コンテンツ鍵ＣＫを暗号化鍵束生成部１０４及び暗号化部１０５へ出力する。なお、コンテンツ鍵ＣＫはコンテンツＣＮＴを暗号化、復号化するための鍵であり、暗号化部１０５及び実行装置１２の実行部１２６で使用される。

【００５８】

（３）実行装置情報格納部１０３

実行装置情報格納部１０３は、複数の実行装置１２に与えられる鍵情報を保持するものである。図３は、実行装置情報格納部１０３の一例を示しており、装置識別子ＡＩＤ１に対応付けられたデバイス鍵ＤＫ１と、装置識別子ＡＩＤ２に対応付けられたデバイス鍵ＤＫ２と、・・・、装置識別子ＡＩＤｓに対応付けられたデバイス鍵ＤＫｓを保持している状態を示している。ここで、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｓのそれぞれは、複数の実行装置１２のいずれかに対応付けられており、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｓのそれぞれは、対応する実行装置１２のデバイス鍵格納部１２２に格納されている鍵である。なお、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｓのそれぞれはコンテンツ鍵ＣＫを暗号化、復号化するための鍵であり、暗号化鍵束生成部１０４及びコンテンツ鍵取得部１２３で用いられる。例えば、装置識別子ＡＩＤ１、ＡＩＤ２、・・・、ＡＩＤｓは、それぞれ異なる自然数１、２、・・・、ｎであり、デバイス鍵ＤＫ１、ＤＫ２、・・・、ＤＫｓは、例えば、それぞれ異なる１２８ビット鍵データである。

【００５９】

（４）暗号化鍵束生成部１０４

暗号化鍵束生成部１０４は、コンテンツ鍵生成部１０２からコンテンツ鍵ＣＫが入力された場合、実行装置情報格納部１０３にアクセスして複数の実行装置１２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢは、各実行装置１２がその暗号化鍵束ＫＢと自身の保持する鍵を用いてコンテンツ鍵ＣＫが取得出来るようなものであればどのようなものでも良い。ここでは、簡単な例を挙げる。まず、各実行装置１２はそれぞれ、ＡＩＤ１からＡＩＤｓのいずれかの装置識別子と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｓのいずれか）を保持しており、実行装置情報格納部１０３には、図３のように、実行装置１２が保持する装置識別子（ＡＩＤ１、・・・、ＡＩＤｓ）と対応するデバイス鍵（ＤＫ１、・・・、ＤＫｓ）の組が全て格納されているとする。そのような場合、暗号化鍵束ＫＢは例えば以下のように生成される。実行装置情報格納部１０３から装置識別子ＡＩＤ１と対応するデバイス鍵ＤＫ１を取得する。そして、デバイス鍵ＤＫ１を基にコンテンツ鍵ＣＫを暗号化し、暗号化コンテンツ鍵ＥＮＣＣＫ１＝Ｅｎｃ（ＤＫ１、ＣＫ）を生成し、装置識別子ＡＩＤ１に対応付ける。なお、Ｅｎｃ（Ｋ、Ｐ）を平文Ｐを暗号化鍵Ｋで暗号化した際の暗号文とし、以後同じ表記を用いる。そして、他の装置識別子（ＡＩＤ２、・・・、ＡＩＤｓ）とデバイス鍵（ＤＫ２、・・・、ＤＫｓ）に対しても同様の処理を行い、暗号化コンテンツ鍵ＥＮＣＣＫ２＝Ｅｎｃ（ＤＫ２、ＣＫ）、・・・、ＥＮＣＣＫｎ＝Ｅｎｃ（ＤＫｓ、ＣＫ）を生成し、装

置識別子ＡＩＤ２、・・・、ＡＩＤｓに対応付ける。そのようにして、装置識別子と対応する暗号化コンテンツ鍵のｓ組から構成される、図４のような暗号化鍵束ＫＢを生成する。暗号化鍵束ＫＢをこのような構成にすることによって、各実行装置１２はその暗号化鍵束ＫＢと自身の保持するデバイス鍵（ＤＫ１、・・、ＤＫｓの何れか）を用いてコンテンツ鍵ＣＫが取得出来るようになる。そして、暗号化鍵束ＫＢを配布部１０９に出力する。なお、特許文献２などに記載の方法を用いることで、暗号化鍵束ＫＢの中の暗号化コンテンツ鍵（先程の例ではｓ個）の数を減らしたり、ある特定の実行装置では正しいコンテンツ鍵ＣＫを取得出来ないようにして、特定の実行装置を無効化することも出来る。また、暗号化鍵束生成部１０４で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、実行装置１２のコンテンツ鍵取得部１２３と同じ暗号アルゴリズムを用いる。

【００６０】

（５）暗号化部１０５

暗号化部１０５は、入力部１０１からコンテンツＣＮＴを入力され、さらに、コンテンツ鍵生成部１０２からコンテンツ鍵ＣＫとが入力された場合、以下のようにして暗号化コンテンツＥＮＣＣＮＴを生成する。ここで、コンテンツＣＮＴは、図５で示すように、ｎ個（ｎは２以上の自然数）の部分コンテンツＣＮＴ＃１、ＣＮＴ＃２、ＣＮＴ＃３、・・・、ＣＮＴ＃ｎから構成されるとする。なお、コンテンツＣＮＴは、初めからｎ個に分割されていているとする。コンテンツＣＮＴが初めからｎ個に分割されている一例としては、コンテンツＣＮＴが複数のファイルから構成されている場合が挙げられる。例えば、コンテンツＣＮＴがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合の、ＶＯＢ（Ｖｉｄｅｏ　ＯＢｊｅｃｔ）ファイル等で分割されており、コンテンツＣＮＴが複数のＭＰＥＧ２形式の動画コンテンツから構成されている場合や、複数のＭＰ３形式の音声コンテンツから構成されている場合もある。なお、ＤＶＤ－Ｖｉｄｅｏ形式については、例えばインターネットアドレスhttp://positron.jfet.org/dvdvideo.htmlに記載されており、ＭＰＥＧ形式については、例えばインターネットアドレスhttp://www.pioneer.co.jp/crdl/tech/mpeg/1.htmlに記載されている。

【００６１】

そして、コンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ＃１を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ＃１＝Ｅｎｃ（ＣＫ、ＣＮＴ＃１）を生成する。続いて、同じコンテンツ鍵ＣＫを用いて部分コンテンツＣＮＴ＃２を暗号化し、暗号化部分コンテンツＥＮＣＣＮＴ＃２＝Ｅｎｃ（ＣＫ、ＣＮＴ＃２）を生成する。これを繰り返して、図５で示すようなｎ個の暗号化部分コンテンツＥＮＣＣＮＴ＃１、・・・、ＥＮＣＣＮＴ＃ｎから構成される暗号化コンテンツＥＮＣＣＮＴを生成する。暗号化部１０５で使用する暗号アルゴリズムは、例えば、非特許文献１に記載のＡＥＳ方式（１２８ビット鍵）などであり、実行装置１２の実行部１２６と同じ暗号アルゴリズムを用いる。ここでは暗号化コンテンツＥＮＣＣＮＴの生成方法として、各部分コンテンツに対して、全て同一のコンテンツ鍵ＣＫで暗号化していたが、非特許文献１に記載のブロック暗号のモードを利用してもよい。例えば、ＣＢＣモードやＯＦＢモード、ＣＦＢモードなどでもよく、さらに、ある一定間隔毎にモード（例：ＣＢＣモード）の初期値を変化させるようにしたものでも良い。

【００６２】

続いて、ｎ個の暗号化部分コンテンツのそれぞれを識別、特定出来る、ｎ個の特定情報ＡＤＤＲ＃１、・・・、ＡＤＤＲ＃ｎを取得する。このｎ個の特定情報は、例えば、暗号化コンテンツＥＮＣＣＮＴが複数のファイルから構成されている場合、各ファイルの先頭の論理アドレスとサイズ、もしくは、先頭と終端の論理アドレス、もしくは、先頭の物理アドレスとサイズ、もしくは、先頭と終端の物理アドレス、などである。ここでは、暗号化部分コンテンツＥＮＣＣＮＴ＃１を識別、特定する情報を特定情報ＡＤＤＲ＃１、暗号化部分コンテンツＥＮＣＣＮＴ＃２を識別、特定する情報を特定情報ＡＤＤＲ＃２、暗号化部分コンテンツＥＮＣＣＮＴ＃３を識別、特定する情報を特定情報ＡＤＤＲ＃３、・・・、暗号化部分コンテンツＥＮＣＣＮＴ＃ｎを識別、特定する情報を特定情報ＡＤＤＲ＃

ｎとする。そして、暗号化コンテンツＥＮＣＣＮＴを配布部１０９へ出力し、暗号化部分コンテンツと特定情報のｎ組｛ＥＮＣＣＮＴ＃１、ＡＤＤＲ＃１｝、｛ＥＮＣＣＮＴ＃２、ＡＤＤＲ＃２｝、・・・、｛ＥＮＣＣＮＴ＃ｎ、ＡＤＤＲ＃ｎ｝を、ヘッダ情報生成部１０６へ出力する。

【００６３】

なお、それぞれの特定情報は、上記で紹介した情報に限らず、各暗号化部分コンテンツを識別、特定出来るものであればどのような情報であっても良い。

【００６４】

（６）ヘッダ情報生成部１０６

ヘッダ情報生成部１０６は、暗号化部１０５から、暗号化部分コンテンツと特定情報のｎ組｛ＥＮＣＣＮＴ＃１、ＡＤＤＲ＃１｝、｛ＥＮＣＣＮＴ＃２、ＡＤＤＲ＃２｝、・・・、｛ＥＮＣＣＮＴ＃ｎ、ＡＤＤＲ＃ｎ｝とが入力された場合、以下のようにして、ヘッダ情報ＨＥＡＤ及びコンテンツ位置情報ＰＯＳを生成する。

【００６５】

ｎ組の暗号化部分コンテンツと特定情報からヘッダ情報ＨＥＡＤを生成する大まかな流れは、図６で示す通りである。まず、ｎ個の暗号化部分コンテンツのそれぞれに対して、第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１、ＨＡＳＨＴＢＬ１＃２、・・・、ＨＡＳＨＴＢＬ１＃ｎを生成する。そして、ｎ個の第一ハッシュテーブル及び特定情報を用いて第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを生成する。

【００６６】

まず、ｎ個の暗号化部分コンテンツのそれぞれに対して、第一ハッシュテーブルを生成する方法について説明する。ここでは例として、暗号化部分コンテンツＥＮＣＣＮＴ＃１から第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１を生成する方法について説明する。なお、暗号化部分コンテンツＥＮＣＣＮＴ＃２、・・・、ＥＮＣＣＮＴ＃ｎから第一ハッシュテーブルＨＡＳＨＴＢＬ１＃２、・・・、ＨＡＳＨＴＢＬ１＃ｎのそれぞれを生成する方法は、暗号化部分コンテンツＥＮＣＣＮＴ＃１から第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１を生成する方法と同じであるため、説明を省略する。まず、図７で示すように、暗号化部分コンテンツＥＮＣＣＮＴ＃１をｍ個（ｍは１以上の自然数）のユニットＵ＃１、Ｕ＃２、・・・、Ｕ＃ｍに分割する。分割する方法の一例としては、例えば暗号化部分コンテンツをある所定の区切り毎に分割する方法がある。ある所定の区切り方の具体例としては、コンテンツデータがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合、例えば、セル（Ｃｅｌｌ）単位などである。コンテンツデータがＭＰＥＧ２形式の動画コンテンツの場合、例えば、ＧＯＰ単位、フィールド単位、フレーム単位、Ｉピクチャ単位などである。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長（ＥＣＣブロック単位）などである。また、コンテンツデータの形式を問わず、例えば、６４キロバイト単位、１メガバイト単位、１秒単位、１分単位などでも良い。そして、ｍ個のユニットのそれぞれを識別可能な第一識別子を取得、もしくは、生成する。第一識別子を取得、もしくは、生成する方法としては、各ユニットを識別可能な論理アドレスや物理アドレスを取得する方法や、自然数を順番に生成し割り当てていく（１、２、・・・、ｍ）方法や、乱数を用いてランダムに割り当てる方法などがある。ここで、各組に対して生成した第一識別子をそれぞれ、ＩＤ１＃１、ＩＤ１＃２、・・・ＩＤ１＃ｍとし、次のように第一識別子とユニットが対応しているとする。｛ＩＤ１＃１、Ｕ＃１｝、｛ＩＤ１＃２、Ｕ＃２｝、・・・、｛ＩＤ１＃ｍ、Ｕ＃ｎ｝。続いて、ｍ組の第一識別子とユニットの各組に対して、ユニットの属性値として第一ハッシュ値を計算する。ユニットの第一ハッシュ値を求める方法としては、例えば一方向性関数を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、実行装置１２の認証情報検証部１２５で用いる方法と同じものを用いる。ここで、各組に対して計算した第一ハッシュ値をそれぞれ、ＨＡＳＨ１＃１、ＨＡＳＨ１＃２、・・・、ＨＡＳＨ１＃ｍとし、次のように第一識別子とユニットと第一ハッシュ値が対応しているとする

。｛ＩＤ１＃１、Ｕ＃１、ＨＡＳＨ１＃１｝、｛ＩＤ１＃２、Ｕ＃２、ＨＡＳＨ１＃２｝、・・・、｛ＩＤ１＃ｍ、Ｕ＃ｍ、ＨＡＳＨ１＃ｍ｝。最後に、その中から第一識別子と第一ハッシュ値を抜き出し、第一ハッシュテーブルＨＡＳＨＴＢＬ＃１＝｛ＩＤ１＃１、ＨＡＳＨ１＃１｝、｛ＩＤ１＃２、ＨＡＳＨ１＃２｝、・・・、｛ＩＤ１＃ｍ、ＨＡＳＨ１＃ｍ｝を生成する。

【００６７】

続いて、ｎ個の第一ハッシュテーブルと対応するｎ個の特定情報を用いて第二ハッシュテーブルＨＡＳＨＴＢＬ２を生成する方法について、図８を用いて説明する。まず、ｎ組の特定情報と第一ハッシュテーブルのそれぞれに対して、第一ハッシュテーブルの属性値として第二ハッシュ値を計算する。第一ハッシュテーブルの第二ハッシュ値を求める方法としては、例えばｍ個の第一ハッシュ値と第一識別子の値を連結した値を一方向性関数に入力した場合の出力値を用いる方法があり、非特許文献１に記載のＳＨＡ－１アルゴリズムやブロック暗号を用いたＣＢＣ－ＭＡＣなどがあり、実行装置１２の認証情報検証部１２５で用いる方法と同じものを用いる。ここで、各組に対して計算した第二ハッシュ値をそれぞれ、ＨＡＳＨ２＃１、ＨＡＳＨ２＃２、・・・、ＨＡＳＨ２＃ｎとし、次のように特定情報と第一ハッシュテーブルと第二ハッシュ値が対応しているとする。｛ＡＤＤＲ＃１、ＨＡＳＨＴＢＬ１＃１、ＨＡＳＨ２＃１｝、｛ＡＤＤＲ＃２、ＨＡＳＨＴＢＬ１＃２、ＨＡＳＨ２＃２｝、・・・、｛ＡＤＤＲ＃ｎ、ＨＡＳＨＴＢＬ１＃ｎ、ＨＡＳＨ２＃ｎ｝。その中から特定情報と第二ハッシュ値を抜き出し、第二ハッシュテーブルＨＡＳＨＴＢＬ２＝｛ＡＤＤＲ＃１、ＨＡＳＨ２＃１｝、｛ＡＤＤＲ＃２、ＨＡＳＨ２＃２｝、・・・、｛ＡＤＤＲ＃ｎ、ＨＡＳＨ２＃ｎ｝を生成する。

【００６８】

最後に、ｎ個の特定情報を用いてコンテンツ位置情報ＰＯＳを生成する方法について、図９を用いて説明する。それぞれの特定情報ＡＤＤＲ＃１、ＡＤＤＲ＃２、・・・、ＡＤＤＲ＃ｎに対して、対応する暗号化部分コンテンツをユニット単位で分割した個数であるユニット数をそれぞれＮＵＭＵ＃１、ＮＵＭＵ＃２、・・・、ＮＵＭＵ＃ｎとする。そして、そのｎ組の特定情報とユニット数から構成される、コンテンツ位置情報ＰＯＳ＝｛ＡＤＤＲ＃１、ＮＵＭＵ＃１｝、｛ＡＤＤＲ＃２、ＮＵＭＵ＃２｝、・・・、｛ＡＤＤＲ＃ｎ、ＮＵＭＵ＃ｎ｝を生成する。

【００６９】

そして、ｎ個の第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１、ＨＡＳＨＴＢＬ１＃２、・・・、ＨＡＳＨＴＢＬ１＃ｎ及び第二ハッシュテーブルＨＡＳＨＴＢＬ２から構成されるヘッダ情報ＨＥＡＤを生成し、コンテンツ位置情報ＰＯＳとともに、配布部１０９へ出力する。また、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを認証情報生成部１０８へ出力する。

【００７０】

（７）認証情報生成情報格納部１０７

認証情報生成情報格納部１０７は、ヘッダ情報ＨＥＡＤの認証情報である認証情報ＡＵＴＨを生成するための、認証情報生成情報ＧＥＮＡＵＴＨを予め与えられ、保持するものである。この認証情報生成情報ＧＥＮＡＵＴＨは、例えば、デジタル署名アルゴリズムの署名生成鍵（秘密鍵）である。認証情報生成情報ＧＥＮＡＵＴＨに対応する検証情報ＶＥＲは、実行装置１２の検証情報格納部１２４に格納されている。この検証情報ＶＥＲは、例えば、デジタル署名アルゴリズムの署名検証鍵（公開鍵）である。デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式やＲＳＡ署名などである。

【００７１】

（８）認証情報生成部１０８

認証情報生成部１０８は、ヘッダ情報生成部１０６から第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳが入力された場合、以下のようにして、認証情報ＡＵＴＨを生成する。まず、認証情報生成情報格納部１０７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、図１０で示すように、第二ハッシュテーブル

ＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳに含まれる値と認証情報生成情報ＧＥＮＡＵＴＨを用いて、認証情報である認証情報ＡＵＴＨを生成する。なお、認証情報ＡＵＴＨの生成方法の一例は、デジタル署名アルゴリズムを用いる方法である。ここでは、デジタル署名アルゴリズムを用いる方法の一例を説明する。まず、第二ハッシュテーブルＨＡＳＨＴＢＬ２に含まれるｎ個の第二ハッシュ値とｎ個の特定情報と、コンテンツ位置情報ＰＯＳに含まれるｎ個の特定情報とｎ個のユニット数を結合した値に対するデジタル署名を作成する。ここで、ＧＥＮＳＩＧ（Ｋ、Ｍ）は署名生成鍵Ｋを用いてメッセージＭに対して生成されたデジタル署名とすると、認証情報ＡＵＴＨは、ＡＵＴＨ＝ＧＥＮＳＩＧ（ＧＥＮＡＵＴＨ、｛ＨＡＳＨ２＃１｜｜ＡＤＤＲ＃１｜｜ＮＵＭＵ＃１｝｜｜｛ＨＡＳＨ２＃２｜｜ＡＤＤＲ＃２｜｜ＮＵＭＵ＃１｝｜｜・・・｜｜｛ＨＡＳＨ２＃ｎ｜｜ＡＤＤＲ＃ｎ｜｜ＮＵＭＵ＃ｎ｝）となる。そして、認証情報ＡＵＴＨを配布部１０９へ出力する。なお、認証情報生成部１０８で使用するデジタル署名アルゴリズムは、実行装置１２の認証情報検証部１２５で用いるデジタル署名アルゴリズムと同じものを用いる。

【００７２】

（９）配布部１０９

配布部１０９は、暗号化鍵束生成部１０４から入力された暗号化鍵束ＫＢと、暗号化部１０５から入力された暗号化コンテンツＥＮＣＣＮＴと、ヘッダ情報生成部１０６から入力されたヘッダ情報ＨＥＡＤ及びコンテンツ位置情報ＰＯＳと、認証情報生成部１０８から入力された認証情報ＡＵＴＨと、を可搬媒体１１へ記録するものである。例えば、可搬媒体１１が書き込み可能な光ディスクであり、配布部１０９は書き込み用レーザー等を用いて該当データを記録する。

【００７３】

＜配布センタ１０の動作＞

以上で、配布センタ１０の構成について説明を行ったが、ここでは配布センタ１０の動作の一例について、図１１に示すフローチャートの処理を行う。なお、配布センタ１０の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理にしても良い。

【００７４】

入力部１０１は、外部から入力されたコンテンツＣＮＴをコンテンツ鍵生成部１０２へ出力し、コンテンツ鍵生成要求ＲＥＱをコンテンツ鍵生成部１０２へ出力する（ステップＳ１０１）。

【００７５】

コンテンツ鍵生成要求ＲＥＱを入力されたコンテンツ鍵生成部１０２は、コンテンツ鍵ＣＫを生成し、コンテンツ鍵ＣＫを暗号化鍵束生成部１０４及び暗号化部１０５へ出力する（ステップＳ１０２）。

【００７６】

コンテンツ鍵ＣＫを入力された暗号化鍵束生成部１０４は、実行装置情報格納部１０３にアクセスして複数の実行装置１２が持つ鍵情報を取得し、その鍵情報とコンテンツ鍵ＣＫとを基に、暗号化鍵束ＫＢを生成する。そして、暗号化鍵束ＫＢを配布部１０９に出力する（ステップ１０３）。

【００７７】

コンテンツＣＮＴ及びコンテンツ鍵ＣＫが入力された暗号化部１０５は、コンテンツ鍵ＣＫを基に、コンテンツＣＮＴを暗号化し、暗号化コンテンツＥＮＣＣＮＴを生成する。そして、暗号化コンテンツＥＮＣＣＮＴを配布部１０９へ出力し、ｎ組の暗号化部分コンテンツと特定情報を、ヘッダ情報生成部１０６へ出力する（ステップＳ１０４）。

【００７８】

ｎ組の暗号化部分コンテンツと特定情報を入力されたヘッダ情報生成部１０６は、ｎ個の第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１、・・・、ＨＡＳＨＴＢＬ１＃ｎと第二ハッシュテーブルＨＡＳＨＴＢＬ２からなるヘッダ情報ＨＥＡＤ、及びコンテンツ位置情報ＰＯＳを生成する。そして、ヘッダ情報ＨＥＡＤ及びコンテンツ位置特定情報ＰＯＳを配

布部１０９へ出力し、さらに、第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳを認証情報生成部１０８へ出力する（ステップＳ１０５）。

【００７９】

第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳを入力された認証情報生成部１０８は、認証情報生成情報格納部１０７にアクセスして、認証情報生成情報ＧＥＮＡＵＴＨを取得する。そして、認証情報生成情報ＧＥＮＡＵＴＨを用いて、第二ハッシュテーブルＨＡＳＨＴＢＬ２とコンテンツ位置情報ＰＯＳに対する認証情報である認証情報ＡＵＴＨを生成する。そして、認証情報ＡＵＴＨを配布部１０９へ出力する（ステップＳ１０６）。

【００８０】

配布部１０９は、入力された暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとを可搬媒体１１へ記録する（ステップＳ１０７）。

【００８１】

以上が、不正コンテンツ検知システム１の構成要素である配布センタ１０の構成と動作である。続いて、可搬媒体１１の構成について説明を行う。

【００８２】

＜可搬媒体１１の構成＞

可搬媒体１１は、例えば、ＤＶＤ－ＲＯＭやＣＤ－ＲＯＭ等のような光ディスクの媒体（メディア）であり、図１２に示すように、暗号化鍵束ＫＢとヘッダ情報ＨＥＡＤとコンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨと暗号化コンテンツＥＮＣＣＮＴとが配布センタ１０によって記録されているものとする。

【００８３】

以上が、不正コンテンツ検知システム１の構成要素である可搬媒体１１の構成である。続いて、実行装置１２の構成と動作について説明を行う。

【００８４】

＜実行装置１２の構成＞

実行装置１２は、図１３に示すように、取得部１２１、デバイス鍵格納部１２２、コンテンツ鍵取得部１２３、検証情報格納部１２４、認証情報検証部１２５、実行部１２６とから構成される。

【００８５】

（１）取得部１２１

取得部１２１は、可搬媒体１１に記録されているデータの読み取りを行う。取得部１２１は、実行装置１２が可搬媒体１１のデータを読み取り可能になった場合に、可搬媒体１１に記録されている暗号化鍵束ＫＢ及びコンテンツ位置情報ＰＯＳ及び認証情報ＡＵＴＨを取得し、暗号化鍵束ＫＢをコンテンツ鍵取得部１２３へ出力し、コンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨを認証情報検証部１２５へ出力する。また、取得部１２１は、認証情報検証部１２５及び実行部１２６からの要求により、可搬媒体１１に記録されているヘッダ情報ＨＥＡＤ及び暗号化コンテンツＥＮＣＣＮＴの全部、もしくは、一部を取得できるものである。

【００８６】

（２）デバイス鍵格納部１２２

デバイス鍵格納部１２２は、配布センタ１０の実行装置情報格納部１０３の中の鍵情報の一部を保持するものであり、デバイス鍵格納部１２２に与えられる鍵情報と暗号化鍵束ＫＢを用いて、コンテンツ鍵ＣＫが取得出来るものである。例えば、実行装置情報格納部１０３が図３のような場合、デバイス鍵格納部１２２には、装置識別子ＡＩＤｉとデバイス鍵Ｋｉ（ｉは１からｓのいずれか）が与えられる。

【００８７】

（３）コンテンツ鍵取得部１２３

コンテンツ鍵取得部１２３は、取得部１２１から暗号化鍵束ＫＢが入力された場合、デバイス鍵格納部１２２に格納されている鍵情報及び暗号化鍵束ＫＢを用いて、コンテンツ

鍵ＣＫを取得する。例えば、暗号化鍵束ＫＢが図４のような場合で、デバイス鍵格納部１２２には装置識別子ＡＩＤｉとデバイス鍵ＤＫｉ（ｉは１からｓのいずれか）が与えられている場合、コンテンツ鍵取得部１２３はデバイス鍵格納部１２２から装置識別子ＡＩＤｉとデバイス鍵ＤＫｉを取得し、暗号化鍵束ＫＢの中から装置識別子ＡＩＤｉに対応する暗号化コンテンツ鍵ＥＮＣＣＫｉ（ＥＮＣＣＫ１からＥＮＣＣＫｓの何れか）を取得する。そしてデバイス鍵ＤＫｉを基に、暗号化コンテンツ鍵ＥＮＣＣＫｉを復号化することによって、コンテンツ鍵ＣＫ＝Ｄｅｃ（ＤＫｉ、ＥＮＣＣＫｉ）を取得する。なお、Ｄｅｃ（Ｋ、Ｃ）は暗号文Ｃを復号化鍵Ｋを用いて復号化した際の復号文とし、以後同じ意味で使用する。そして、コンテンツ鍵ＣＫを実行部１２６へ出力する。

【００８８】

（４）検証情報格納部１２４

検証情報格納部１２４は、認証情報ＡＵＴＨの正当性を検証するために必要な検証情報ＶＥＲを保持するものである。この検証情報ＶＥＲに対応する認証情報生成情報ＧＥＮＡＵＴＨは、配布センタ１０の認証情報生成情報格納部１０７に格納されている。例えば、検証情報ＶＥＲはデジタル署名アルゴリズムの署名検証鍵（公開鍵）である。

【００８９】

（５）認証情報検証部１２５

認証情報検証部１２５は、コンテンツ位置情報ＰＯＳ及び認証情報ＡＵＴＨが入力された場合、認証情報ＡＵＴＨの正当性を検証する。検証は以下のように行われる。

【００９０】

まず、図１４で一例を示すように、コンテンツ位置情報ＰＯＳに含まれるｎ組の特定情報ＡＤＤＲ＃１、・・・、ＡＤＤＲ＃ｎとユニット数Ｕ＃１、・・・、Ｕ＃ｎから、ｉ組（ｉは１以上ｎ－１以下の自然数）の特定情報とユニット数を選択する。ここで、選択されたｉ組の特定情報とユニット数からなるデータを被選択コンテンツ位置情報とする。ここでは、第三者によってどの特定情報とユニット数が選択されるか推測できないようにする。この方法は、例えば真性乱数や擬似乱数を用いることにより実現出来る。真性乱数は、例えばノイズなどを利用することにより発生出来る。擬似乱数は、例えば擬似乱数生成アルゴリズムとシードを用いることにより発生出来る。これらは共に、認証情報検証部１２５が乱数生成器を有することにより実現出来る。これら乱数を生成する方法については、非特許文献２が詳しい。なお、乱数生成器を利用しなくても、推測出来ない情報であれば何でも良い。例えば、気温や湿度などでも良い。これは、認証情報検証部１２５が温度センサや湿度センサを有することにより実現出来る。

【００９１】

続いて、図１５で示すように、選択されたｉ組の特定情報とユニット数（被選択コンテンツ位置情報）、及び、可搬媒体１１に記録されている第二ハッシュテーブルＨＡＳＨＴＢＬ２の一部を基に、入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する。入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する方法は、以下の通りである。まず、選択されたｉ組の特定情報とユニット数のそれぞれに対応するｉ個の入替第一ハッシュテーブルを生成する。ここでは、選択されたｉ組の特定情報とユニット数のうち、１組が特定情報ＡＤＤＲ＃１とユニット数ＮＵＭＵ＃１である場合を例に挙げ、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１を生成する手順について説明する。なお、他の特定情報とユニット数の場合であっても、同様の手順となる。まず、ユニット数ＮＵＭＵ＃１を基に、特定情報ＡＤＤＲ＃１に対応する暗号化部分コンテンツＥＮＣＣＮＴ＃１に含まれるユニットの数を認識し、１番目からｄ番目（ｄはユニット数ＮＵＭＵ＃１）までのユニットのうち、ｊ個（ｊは１以上ｍ以下の自然数）のユニットを選択する。ここでも、第三者によってどのユニットが選択されるか推測できないようにする。この方法は、先ほど、コンテンツ位置情報ＰＯＳに含まれるｎ組の特定情報とユニット数から、ｉ組の特定情報とユニット数を選択する方法と同様の方法が利用可能であるため、説明を省略する。以後、説明を簡略化するために、ｊは１とし、図１６で示すように、ユニットＵ＃３（図１６における横点線）が選択されたとする。そして、そのユニットＵ＃３に対する属

性値である第一ハッシュ値Ｈ１（図１６における縦線）を計算する。また、特定情報ＡＤＤＲ＃１及びユニット数Ｕ＃３を基に、取得部１２１経由で可搬媒体１１からＩＤ１＃３以外の選択されなかった第一識別子に対応する第一ハッシュ（図１６における横点線）を取得する。そして、選択された第一識別子に対応するユニットの属性値を計算することによって取得した第一ハッシュ値、及び、選択されなかった第一識別子に対応する第一ハッシュ値から構成される、図１６で示される、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１を生成する。

【００９２】

続いて、生成されたｉ個の入替第一ハッシュテーブル、及び、可搬媒体１１に記録されている第二ハッシュテーブルＨＡＳＨＴＢＬ２の一部を基に、入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する方法について説明する。図１７で一例を示すように、まず、ｉ個の入替第一ハッシュテーブルのそれぞれに対する属性値として、第二ハッシュ値（図１７における縦線）を生成する。図１７では、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１に対する属性値として第二ハッシュ値Ｈ２＃１、・・・、入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃ｃに対する属性値として第二ハッシュ値Ｈ２＃ｃとしている。次に、選択されなかった特定情報に対応する第二ハッシュ値を、取得部１２１経由で可搬媒体１１から取得する（図１７における横点線）。そして、入替第一ハッシュテーブルの属性値を計算することによって取得した第二ハッシュ値、及び、選択されなかった特定情報に対応する第二ハッシュ値から構成される、図１７で示される、入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２を生成する。

【００９３】

最後に、検証情報格納部１２４に格納されている検証情報ＶＥＲを使って、図１８で示すように、認証情報ＡＵＴＨが発行センタ１０による入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳに対する正規の認証情報であるかを検証する。例えば、デジタル署名検証アルゴリズムを用いて、認証情報ＡＵＴＨが正しいデジタル署名であるかを検証する。このデジタル署名検証アルゴリズムは、配布センタ１０の認証情報生成部１０８で用いるデジタル署名生成アルゴリズムと同じデジタル署名アルゴリズムを用いる。なお、デジタル署名アルゴリズムは、例えば、非特許文献１に記載のＤＳＡ方式などである。認証情報検証部１２５は、認証情報ＡＵＴＨが発行センタ１０による正しい認証情報である場合にのみ、実行開始許可情報ＰＥＲＭを実行部１２６へ出力する。なお、被選択コンテンツ位置情報に含まれるｉ個の特定情報に対応するｉ個の暗号化部分コンテンツを、被選択部分コンテンツとする。

【００９４】

（６）実行部１２６

実行部１２６は、コンテンツ鍵取得部１２３からコンテンツ鍵ＣＫが入力され、かつ、認証情報検証部１２５から実行開始許可情報ＰＥＲＭが入力された場合に、取得部１２１経由で、可搬媒体１１に記録されている暗号化コンテンツＥＮＣＣＮＴを逐次取得し、逐次コンテンツ鍵ＣＫを基に復号化を行って、逐次実行するものである。例えば、実行部１２６はＭＰＥＧ２データやＭＰ３データをデコードする機能を有するデコータを有していて、ＭＰＥＧ２形式の動画コンテンツやＭＰ３形式の音声コンテンツであるコンテンツＣＮＴを逐次デコードして、外部に出力するものである。また、例えば、実行部１２６は、ディスプレイやスピーカーを備えて動画コンテンツや音声コンテンツを再生するようなものでも良いし、別の可搬媒体や記録媒体にコンテンツデータを出力するようなものでも良いし、印刷機能を有しコンテンツデータを紙などに印刷するようなものでもよい。

【００９５】

＜実行装置１２の動作＞

以上で、実行装置１２の構成について説明を行ったが、ここで実行装置１２の動作について、図１９に示すフローチャートを用いて説明する。なお、実行装置１２の動作に関しては、所望の結果が得られれば、各処理をどのような順番で行っても構わない。さらには、いくつかの処理を並列処理しても良い。

【００９６】
実行装置１２が可搬媒体１１のデータを読み取り可能になった場合に、取得部１２１は可搬媒体１１に記録されている暗号化鍵束ＫＢ及びコンテンツ位置情報ＰＯＳ及び認証情報ＡＵＴＨを取得し、暗号化鍵束ＫＢをコンテンツ鍵取得部１２３へ出力し、コンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨを認証情報検証部１２５へ出力する（ステップＳ１２１）。

【００９７】
暗号化鍵束ＫＢを入力されたコンテンツ鍵取得部１２３は、デバイス鍵格納部１２２が保持している鍵情報を用いて、コンテンツ鍵ＣＫを取得する。そして、コンテンツ鍵ＣＫを実行部１２６へ出力する（ステップＳ１２２）。

【００９８】
コンテンツ位置情報ＰＯＳと認証情報ＡＵＴＨを入力された認証情報検証部１２５は、検証情報格納部１２４に格納されている検証情報ＶＥＲを使って、認証情報ＡＵＴＨが発行センタ１０による正規の認証情報であるかを検証する（ステップＳ１２３）。

【００９９】
認証情報検証部１２５は、認証情報ＡＵＴＨが発行センタ１０による正しい認証情報である場合にのみ、実行開始許可情報ＰＥＲＭを実行部１２６へ出力し、ステップＳ１２５へ進む。もし、認証情報ＡＵＴＨが正しい認証情報ではない場合、処理を終了する（ステップＳ１２４）。

【０１００】
コンテンツ鍵ＣＫ及び実行開始許可情報ＰＥＲＭを入力された実行部１２６は、取得部１２１経由で、可搬媒体１１に記録されている暗号化コンテンツＥＮＣＣＮＴを逐次取得し、逐次コンテンツ鍵ＣＫを基に復号化を行って、逐次実行する（ステップＳ１２５）。

【０１０１】
以上が、不正コンテンツ検知システム１の構成要素である実行装置１２の構成と動作である。尚、デバイス鍵格納部１２２、コンテンツ鍵取得部１２３、検証情報格納部１２４、認証情報検証部１２５、等の各機能ブロックは典型的には集積回路であるＬＳＩとして実現されていてもよい。これらは個別に１チップ化されても良いし、一部又は全てを含むように１チップ化されても良い。

【０１０２】
ここでは、ＬＳＩとしたが、集積度の違いにより、ＩＣ、システムＬＳＩ、スーパーＬＳＩ、ウルトラＬＳＩと呼称されることもある。

【０１０３】
また、集積回路化の手法はＬＳＩに限るものではなく、専用回路又は汎用プロセサで実現してもよい。ＬＳＩ製造後に、プログラムすることが可能なＦＰＧＡ（Ｆｉｅｌｄ　Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）や、ＬＳＩ内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサーを利用しても良い。

【０１０４】
さらには、半導体技術の進歩又は派生する別技術によりＬＳＩに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

【０１０５】
＜不正コンテンツ検知システム１の効果＞
以上、不正コンテンツ検知システム１について実施の形態に基づいて説明したが、この不正コンテンツ検知システム１においては、配布センタ１０が、暗号化されたコンテンツＣＮＴとともに、ヘッダ情報ＨＥＡＤ、及び、コンテンツ位置情報ＰＯＳ、及び、認証情報ＡＵＴＨ（例えばデジタル署名）を可搬媒体１１に記録するようにして、実行装置１２では、コンテンツＣＮＴの実行、再生開始前に、認証情報ＡＵＴＨが正規の認証情報（例えばデジタル署名）であるか検証する際に、コンテンツ位置情報ＰＯＳを基にヘッダ情報ＨＥＡＤに含まれるハッシュ値のうち、一部のハッシュ値に絞って検証するようにした。

ここでは、コンテンツＣＮＴを実行、再生開始する毎に、異なるハッシュ値を選択するようにして、不正者は、どのハッシュ値が選択されるか予想出来ないように注意する。そして、選択された一部のハッシュ値が共に正当であると検証された場合にのみ、コンテンツＣＮＴの実行、再生を開始するようにした。そうすることにより、実行装置１２は、不正な認証情報ＡＵＴＨもしくはヘッダ情報ＨＥＡＤもしくはコンテンツ位置情報ＰＯＳもしくは暗号化コンテンツＥＮＣＣＮＴが記録された可搬媒体１１のコンテンツＣＮＴは実行開始しないようになる。これにより、コンテンツＣＮＴの中のある部分コンテンツを不正な部分コンテンツに差し替えようとしても、その不正な部分コンテンツに差し替えられた部分に対応するハッシュ値の検証が行われた場合、そのコンテンツは実行出来なくなる。つまり、コンテンツＣＮＴの一部分でも不正な部分コンテンツに差し替えた場合、ある確率でコンテンツＣＮＴを実行できなくなることになる。これは、コンテンツＣＮＴの中の一部分を、不正なコンテンツに差し替えられるような攻撃を防ぐ抑止力となる。

【０１０６】

さらに、実行装置１２は、認証情報ＡＵＴＨの正当性の検証を、コンテンツＣＮＴを実行、再生開始する前に全て行うため、コンテンツＣＮＴの実行、再生中の特別な処理が必要なくなり、従来例に比べ、コンテンツＣＮＴの実行中の処理負荷が軽減されるという効果を有する。

【０１０７】

さらに、第一ハッシュテーブルと第二ハッシュテーブルというハッシュの２層構造にすることによって、実行装置１２では、認証情報ＡＵＴＨの検証時に、可搬媒体１１から全ての第一ハッシュ値を取得する必要がなくなった。これにより、可搬媒体から取得しなくてはならないハッシュ値の数を少なくすることが出来、実行装置１２の処理時間を短くすることが出来る。

【０１０８】

また、さらに、実行装置１２では、認証情報ＡＵＴＨを用いて、コンテンツ位置情報ＰＯＳの正当性を検証するようにした。これにより、可搬媒体１１におけるファイルシステム等を操作することによって、実行装置１２の認証情報検証部１２５において選択対象となる特定情報及びユニットの数を意図的に少なくするような攻撃に耐性を持たせることが出来るようになった。実行装置１２の認証情報検証部１２５において選択対象となる特定情報及びユニットの数を意図的に少なく出来る場合、その選択対象外となった特定情報及びユニットに対応するコンテンツを不正コンテンツに差し替えることが可能となる。そのため、コンテンツ位置情報ＰＯＳの正当性を検証することは、実行装置１２の認証情報検証部１２５において選択対象となる特定情報及びユニットの数を意図的に少なく出来ないという面で効果がある。

【０１０９】

また、さらに、実行装置１２では、コンテンツを実行、再生開始する場合に、暗号化コンテンツの一部分の属性値（ハッシュ値）を検証するようにした。これにより、従来技術のように、暗号化コンテンツを一度復号化して属性値を検証する場合に比べ、処理時間を短縮することが出来た。

【０１１０】

＜変形例＞

上記に説明した実施の形態は、本発明の実施の形態の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において主な態様で実施し得るものである。以下のような場合も本発明に含まれる。

【０１１１】

（１）実施の形態１の認証情報ＡＵＴＨは、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを連結した値に対する認証情報であったが、これに限るものではない。例えば、第二ハッシュテーブルＨＡＳＨＴＢＬ２に含まれるｎ個の第二ハッシュ値とコンテンツ位置情報ＰＯＳに含まれるｎ個の特定情報とｎ個のユニット数を連結した値に対する認証情報であっても良い。また、第二ハッシュテーブルＨＡＳＨＴＢＬ２に

含まれるｎ個の第二ハッシュ値とコンテンツ位置情報ＰＯＳに含まれるｎ個のユニット数を連結した値に対する認証情報であっても良い。

【０１１２】

（２）実施の形態１の認証情報ＡＵＴＨは、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳを連結した値に対する認証情報であったが、これに限るものではない。例えば、第二ハッシュテーブルＨＡＳＨＴＢＬ２及びコンテンツ位置情報ＰＯＳに加え、コンテンツ鍵ＣＫを連結した値に対する認証情報であっても良い。こうすることにより、コンテンツ鍵ＣＫを持たないものは、認証情報ＡＵＴＨの正当性すら検証出来なくなり、安全性がより高まる。

【０１１３】

（３）実施の形態１の可搬媒体１１では、暗号化コンテンツＥＮＣＣＮＴが記録されていたが、可搬媒体１１には、暗号化されていないコンテンツＣＮＴをそのまま記録するようにしても良い。こうすることにより、実行装置１２で暗号化コンテンツＥＮＣＣＮＴを復号化する必要がなくなるという効果が生まれる。

【０１１４】

（４）実施の形態１の配布センタ１０は、図２で示すような構成に限るものではない。例えば、認証情報ＡＵＴＨなどを可搬媒体１１へ記録する配布部１０９と、ヘッダ情報ＨＥＡＤに対する認証情報を生成する認証情報生成部１０８とを、別の主体が行うようにしても良い。例えば、コンテンツＣＮＴに対する認証情報を生成するのはコンテンツＣＮＴの正規の著作権者であり、認証情報ＡＵＴＨなどを可搬媒体１１へ記録するのはディスク製造業者であるなど、が考えられる。

【０１１５】

（５）実施の形態１の配布センタ１０の認証情報生成情報格納部１０７、及び、実行装置１２の検証情報格納部１２５は、これに限るものではない。例えば、以下のような例が考えられる。

【０１１６】

（ｉ）一つの例として、認証情報生成情報格納部１０７は、図２０で示すように、１つの認証情報生成情報ＧＥＮＡＵＴＨｉ（ＧＥＮＡＵＴＨ１、・・・、ＧＥＮＡＵＴＨｗのいずれか（ｗは１以上の自然数））と対応する検証情報識別子ＶＥＲＩＤｉを保持しており、検証情報格納部１２５は、図２１で示すように、ｗ組の検証情報識別子（ＧＥＮＡＵＴＨ１、・・・、ＧＥＮＡＵＴＨｗ）と、その検証情報識別子に対応する認証情報生成情報と対となる検証情報（ＶＥＲ１、・・・、ＶＥＲｗ）を保持している場合が考えられる。この場合、配布センタ１０の配布部１０９は、可搬媒体１１に、認証情報生成情報格納部１０７に格納されている検証情報識別子ＧＥＮＡＵＴＨｉを加えて記録するようにして、さらに、実行装置１２の認証情報検証部１２６は、可搬媒体１１に記録されている検証情報識別子ＧＥＮＡＵＴＨｉに対応する検証情報ＶＥＲｉ（ＶＥＲ１、・・・、ＶＥＲｗのいずれか）を検証情報格納部１２５から取得し、その検証情報ＶＥＲｉを基に、認証情報ＡＵＴＨを検証することになる。

【０１１７】

（ｉｉ）別の例として、認証情報生成情報格納部１０７には、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲを保持しており、検証情報格納部１２５には、何も保持してない場合が考えられる。この場合、配布センタ１０の配布部１０９は、可搬媒体１１に、認証情報生成情報格納部１０７に格納されている検証情報ＶＥＲを加えて記録するようにして、さらに、実行装置１２の認証情報検証部１２６は、可搬媒体１１に記録されている検証情報ＶＥＲを基に、認証情報ＡＵＴＨを検証することになる。

【０１１８】

（ｉｉｉ）さらなる別の例として、認証情報生成情報格納部１０７には、図２２で示すように、認証情報生成情報ＧＥＮＡＵＴＨと対応する検証情報ＶＥＲ、及び、第三者機関によって生成された検証情報ＶＥＲに対する認証情報（例えばセンタによるデジタル署名）であるセンタ認証情報ＣＡＵＴＨを保持しており、検証情報格納部１２５は、図２３で

示すように、第三者機関の検証情報であるセンタ検証情報ＣＶＥＲ（例えばセンタのデジタル署名の署名検証鍵）を保持している場合が考えられる。なお、第三者機関の具体例としては、信頼出来る第三者機関（Ｔｒｕｓｔｅｄ　Ｔｈｉｒｄ　Ｐａｒｔｙ）や、鍵配布センタなどである。この場合、配布センタ１０の配布部１０９は、可搬媒体１１に、認証情報生成情報格納部１０７に格納されている検証情報ＶＥＲ及びセンタ認証情報ＣＡＵＴＨを加えて記録するようにして、さらに、実行装置１２の認証情報検証部１２６は、検証情報格納部１２５のセンタ検証情報ＣＶＥＲを用いて、可搬媒体１１に記録されているセンタ認証情報ＣＡＵＴＨが、検証情報ＶＥＲに対する第三者機関の正規の認証情報であるかどうか検証し、その検証が成功した場合に、その検証情報ＶＥＲを基に、認証情報ＡＵＴＨを検証するようにすることになる。

【０１１９】

このようにすることによって、配布センタ１０が複数存在している場合にそれぞれの配布センタ１０に別の検証情報を設定したとしても、実行装置１２に予め各検証情報を保持しておく必要がなくなる。

【０１２０】

（６）変形例（５）において、実行装置１２は、さらに、無効検証情報を外部から受信するようにしてもよい。例えば、変形例（５）の（ｉ）の場合、無効検証情報には、検証情報識別子が含まれており、実行装置１２には、外部から無効検証情報として検証情報識別子ＧＥＮＡＵＴＨｊを受信した場合に、検証情報格納部１２５に格納されている検証情報識別子ＧＥＮＡＵＴＨｊに対応する検証情報ＶＥＲｊを無効化する検証情報無効化部を備えていてもよい。

【０１２１】

また、変形例（５）の（ｉｉ）及び（ｉｉｉ）の場合、無効検証情報には、検証情報が含まれており、実行装置１２の検証情報格納部１２５は、外部から受信した無効検証情報として検証情報を保持しており、認証情報検証部１２６は、検証情報格納部１２５の無効検証情報に、可搬媒体１１に記録されている検証情報が含まれていないか確認を行い、含まれている場合は、コンテンツＣＮＴの実行開始を行わないようにしてもよい。

【０１２２】

なお、実行装置１２が外部から無効検証情報を受信する方法としては、可搬媒体１１や記録媒体に記録されている無効検証情報を受信する方法や、通信ネットワークや放送網から無効検証情報をダウンロードする方法などがある。このようにすることによって、万が一、ある配布センタの認証情報生成情報が不正者に漏洩したとしても、その認証情報生成情報に対応する検証情報を無効検証情報に含めることによって、その漏洩した認証情報生成情報を無効化することが実現出来る。

【０１２３】

（７）変形例（６）において、実行装置１２は、最新の無効検証情報のみを検証情報格納部１２５に保持するようにしてもよい。例えば、無効検証情報には発行日が記載されており、実行装置１２は、検証情報格納部１２５が保持する無効検証情報よりも発効日が新しい無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部１２５に上書きするようにしてもよいし、また、無効検証情報には発行ＩＤが記載されており、実行装置１２は、検証情報格納部１２５が保持する無効検証情報よりも発行ＩＤが最新の無効検証情報を受信した場合にのみ、受信した無効検証情報を検証情報格納部１２５に上書きするようにしてもよい。

【０１２４】

（８）実施の形態１のコンテンツＣＮＴは、動画データや音声データなどのコンテンツであったが、コンピュータプログラムであっても良い。この場合、実行装置１２は、コンピュータプログラムを実行するために必要なＣＰＵやメモリ、ディスクなどを備えていれば良い。こうすることにより、実行装置１２では、不正なコンピュータプログラムを実行開始しないようになるため、コンピュータウイルス等を防ぐ対策として有効となる。

【０１２５】

（９）実施の形態１の配布センタ１０では、コンテンツ鍵生成部１０２においてコンテンツ鍵ＣＫを生成していたが、配布センタ１０が一以上のコンテンツ鍵ＣＫを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵生成部１０２はコンテンツ鍵格納部からいずれかのコンテンツ鍵ＣＫを取得するようにしても良い。こうすることにより、コンテンツ鍵ＣＫを予めまとめて作成しておくことが出来る。

【０１２６】

（１０）実施の形態１の実行装置１２のコンテンツ鍵取得部１２３では、暗号化鍵束ＫＢ、及びデバイス鍵格納部１２２に格納されている情報を用いて、コンテンツ鍵ＣＫを取得していたが、配布センタ１０がデバイス鍵格納部１２２の替わりに、コンテンツ鍵ＣＫを保持するコンテンツ鍵格納部を有していて、コンテンツ鍵取得部１２３はコンテンツ鍵格納部からコンテンツ鍵を取得するようにしても良い。この場合、発行センタ１０は可搬媒体１１に暗号化鍵束ＫＢを記録する必要はなく、実行装置１２は暗号化鍵束ＫＢを受信する必要もない。こうすることにより、可搬媒体１１に暗号化鍵束ＫＢを記録しなくてすむため、記録データのサイズを削減することが出来る。

【０１２７】

（１１）実施の形態１において、配布センタ１０は、可搬媒体１１を介して実行装置１２へコンテンツＣＮＴに関する情報を配布していたが、これに限るものではない。例えば、配布センタ１０と実行装置１２がインターネット等の通信ネットワークに接続されており、配布センタ１０は、その通信ネットワークを介して実行装置１２へコンテンツＣＮＴに関する情報を配布してもよいし、他にも通信ネットワークが放送網であってもよい。

【０１２８】

（１２）実施の形態１において、実行装置１２は可搬媒体１１内のコンテンツＣＮＴを実行開始する前に、そのコンテンツＣＮＴが不正なものであるか検証していたが、それに限るものではない。例えば、可搬媒体１１が光ディスクであり、実行装置１２がディスクトレイを有している場合、可搬媒体１１が実行装置１２のディスクトレイに挿入された場合に、そのコンテンツＣＮＴが不正なものであるか検証するようにしても良い。そうすることにより、ディスクトレイに挿入された可搬媒体１１内のコンテンツＣＮＴをイジェクトせずに何度も実行、再生する場合にでも、光ディスクの挿入時１度しか検証しないですむようになるため、コンテンツＣＮＴの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体１１がＳＤカード等の外部メモリで、実行装置１２が外部メモリスロットを有している場合にも、同様のことが実現出来る。

【０１２９】

（１３）実施の形態１の実行装置１２の認証情報検証部１２５においては、入替第二ハッシュテーブルを生成し、それを基に認証情報ＡＵＴＨの正当性を検証していたが、これに限るものではない。例えば、実行装置１２の認証情報検証部１２５では、まずステップ１として、図２４で示すように、可搬媒体１１に記録されていた認証情報ＡＵＴＨが、同じく可搬媒体１１に記録されていた第二ハッシュテーブル及びコンテンツ位置情報の正規の認証情報であるか検証し、次にステップ２として、図２５で示すように、選択された特定情報に対応する暗号化部分コンテンツの属性値が、特定情報に対応する第二ハッシュ値と等しいかどうか検証し、さらに、選択された第一識別子に対応するユニットの属性値が、第一識別子に対応する第一ハッシュ値と等しいかどうか検証するようにしてもよい。これにより、同様にコンテンツの正当性を検証することが出来る。暗号化部分コンテンツの属性値と第二ハッシュ値との検証については、図２６に詳細を示している。また、ユニットの属性値と第一ハッシュ値との検証については、図２７に詳細を示している。

【０１３０】

（１４）実施の形態１において、可搬媒体１１にはヘッダ情報ＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴとをそれぞれ一つずつ格納していたが、これに限るものではない。例えば、可搬媒体１１にはヘッダ情報ＨＥＡＤと暗号化コンテンツＥＮＣＣＮＴをそれぞれｚ個（ｚは２以上の自然数）格納しても良い。このような場合、以下のようなことが実現出来る。ここでは、例えば、可搬媒体１１が光ディスクであり、実行装置１２はディスクト

レイを有しているとする。この場合、可搬媒体１１が実行装置１２のディスクトレイに挿入された時に、全てのヘッダ情報の中のコンテンツ位置情報からいくつかの特定情報を選択し検証を行うようにする。そして、複数あるコンテンツの中の一つのコンテンツを実行、再生開始する前に、そのコンテンツに対応するヘッダ情報の中のコンテンツ位置情報の中からいくつかの特定情報を選択し検証を行うようにしても良い。つまり、可搬媒体１１が実行装置１２のディスクトレイに挿入された場合に一度のみ、多くの数の特定情報の検証を行い、各コンテンツを実行、再生開始する際には、ディスクトレイに挿入された時よりも少ない数の特定情報に対して検証するようにする。これにより、ディスクトレイに挿入された可搬媒体１１内のコンテンツを何度も実行する場合に、コンテンツの実行、再生開始までの処理時間を短く出来るという利点が生まれる。なお、可搬媒体１１は光ディスク出なくてもよく、例えばＳＤカード等の外部メモリであっても同様のことが実現出来る。

【０１３１】

（１５）実施の形態１においては、実行装置１２の認証情報検証部１２５では、検証が成功した場合にのみ、実行部１２６へ実行許可情報ＰＥＲＭを出力していたが、これに限るものではない。例えば、実行部１２６は、コンテンツ鍵取得部１２３からコンテンツ鍵を入力された場合に、可搬媒体１１に記録された暗号化コンテンツを逐次取得、復号化、実行するようにして、認証情報検証部１２５は、検証が失敗した場合に、実行部１２６へ実行不許可情報ＮＯＴＰＥＲＭを出力するようにしてもよい。こうすることにより、コンテンツを実行開始するまでの時間を短縮することが出来るようになる。

【０１３２】

また、実行装置１２の認証情報検証部１２５では、検証が成功した場合に実行部１２６へ実行許可情報ＰＥＲＭを出力し、検証が失敗した場合に実行部１２６へ実行不許可情報ＮＯＴＰＥＲＭを出力するようにしてもよい。その際、実行不許可情報ＮＯＴＰＥＲＭを入力された実行部１２６では、外部に不正なコンテンツである旨メッセージを出力（例えば、ディスプレイに「不正なコンテンツです」と表示する）するようにしても良い。その際、実行不許可情報ＮＯＴＰＥＲＭを入力された実行部１２６では、暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を停止するのではなく、暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生は通常通り行うが、同時に外部に警告を出力（例えば、ディスプレイに「警告：不正なコンテンツです」と表示する）するようにしても良い。また、実行装置１２とサーバ（配布センタ１０や別のセンタ）とが通信ネットワーク等で接続されていて、不正コンテンツである旨をそのサーバに通知するようにしてもよい。また、実行装置１２では以後、あらゆる暗号化コンテンツＥＮＣＣＮＴの復号化及び実行、再生を禁止するような状態になってもよい。また、実行装置１２は、不正コンテンツを識別するコンテンツ識別情報（例えば、コンテンツ識別子）を装置内に記録するようにして、一定期間内、もしくは、永久的に、コンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、実行装置１２は、同じコンテンツ識別情報（例えば、コンテンツ識別子）を持つコンテンツがある一定回数以上認証に失敗した場合、一定期間内、もしくは、永久的に、そのコンテンツ識別情報に対応するコンテンツが入力された場合に、無条件で実行、再生を禁止するようにしてもよい。また、可搬媒体１１が光ディスクであり、実行装置１２がディスクトレイを有している場合、可搬媒体１１がディスクトレイから排出されるようにしても良い。

【０１３３】

（１６）実施の形態１において、実行装置１２の認証情報検証部１２５は、可搬媒体１１から複数のユニットを取得する場合、アクセス時間の高速化を目的に、ユニットを取得する順番を最適化するようにしても良い。

【０１３４】

ここでは一例として、以下のような状況を想定する。実行装置１２の認証情報検証部１２５は、４個のユニットＵ＃１、Ｕ＃２、Ｕ＃３、Ｕ＃４を取得したいとする。また、可搬媒体１２は、ＣＤ－ＲＯＭやＤＶＤ－ＲＯＭなどの光ディスクであるとする。その可搬

媒体１２（光ディスク）上には、データを記録する部分がいくつかに分かれており、年輪状に広がっている各領域をトラックと呼ぶ。各トラックには、いくつかのセクタを含み、データはセクタ単位で読み書きされる。例えば、１セクタのサイズは５１２バイトである。このような場合、可搬媒体１２上の読み取り対象データは、トラック識別番号やセクタ識別番号やセクタサイズにより特定することが出来る。取得部１２１は、ヘッド機構部（ピックアップ）及び回転軸を備え、回転軸により可搬媒体１１（光ディスク）を半時計回りに回転させるものとする。ヘッド機構部（ピックアップ）から特定情報（トラック識別番号やセクタ識別番号やセクタサイズ）を指定することで、対象部分のデータを取得出来るものとする。ここでは、４個のユニットＵ＃１、Ｕ＃２、Ｕ＃３、Ｕ＃４は、図２８のように可搬媒体１２（光ディスク）上の位置に記録されているとし、可搬媒体１１（光ディスク）とヘッド機構部も、図２８で示す場所に存在しているとする。ここで、一般に、該当読取位置に対応するトラック位置へヘッド機構部（ピックアップ）を移動させる時間がかかることが知られている。言い換えると、可搬媒体１１（光ディスク）上における内周のトラックから外周方向への移動、もしくは、外周のトラックから内周方向への移動に大きな処理時間がかかることに起因している。可搬媒体１１（光ディスク）上における内側のトラック上にあるデータを読み込んだ後に、外側のトラック上にあるデータを読み込み、その後、また内側のトラック上にあるデータを読み込む場合がその一例である。

【０１３５】

上記のような状況の場合、実施の形態１の動作に沿えば、まず１番目に、ユニットＵ＃１の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後、２番目にユニットＵ＃２の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。その後も同様に、ユニットＵ＃３の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得し、最後に、ユニットＵ＃４の読取位置まで到着するまでヘッド機構部を移動させてから、該当データを取得する。つまり、ユニットＵ＃１を取得するまでに、ヘッド機構部を内周から外周へ移動させ、続いて、ユニットＵ＃２を取得するまでに、ヘッド機構部を外周から内周へ移動させる。その後も、ユニットＵ＃３を取得するまでに、ヘッド機構部を内周から外周へ移動させ、最後に、ユニットＵ＃４を取得するまでに、ヘッド機構部を外周から内周へ移動させる。つまり、４つのデータを取得するまでに、ヘッダ機構部を何度も移動往復させる必要があることが分かる。

【０１３６】

そこで、本変形例では、上記全４つのデータの取得時間を短くする目的で、実行装置１２の認証情報検証部１２５は、まずはじめに、それぞれのデータを取得する順序の最適値を計算する。例えば、一番初めに一番内側のトラック上にあるデータを全て取得して、その次に、一つ外側のトラック上にあるデータを全て取得いく、というようなことを繰り返す。この場合、トラック上に一つもデータがない場合は、そのトラックをスキップして次のトラックに進むようにする。例えば、４つのユニットが図２８のように可搬媒体１２（光ディスク）上の位置に記録されているとし、さらに、可搬媒体１１（光ディスク）及びヘッド機構部（ピックアップ）が図２８で示す場所に存在しているとする。すると、このデータを取得する順序の最適値は、内周側から外周側に向かって、ユニットＵ＃２、ユニットＵ＃４、ユニットＵ＃３、ユニットＵ＃１となる。このようにすることで、可搬媒体１１（光ディスク）上に記録されているとびとびの部分データをランダムに取得する（いわゆるランダムアクセス）場合にでも、取得したい全てのデータを取得するまでの時間を短縮することが出来る。なお、当然、ユニットは４個以外であっても適用可能である。

【０１３７】

なお、最適化手段は、取得部１２１（ヘッド機構部や回転軸等）の動作の特徴に依存するため、本変形例で説明した最適化手段は、あくまで一例であることを注意しておく。例えば、光ディスクの回転制御方式には、角速度一定方式や線速度一定方式があり、これらの特徴を考慮するようにしても良い。また、可搬媒体１１は当然光ディスクでなくてもよく、例えばハードディスクなどでも同様のことが実現出来る。

【０１３８】
（１７）実施の形態１において、認証情報検証部１２５は、予め実行装置１２に与えられているパラメータｉ、ｊに従って検証を実施していたが、これに限るものではない。例えば、配信装置１０は可搬媒体１１に、パラメータｉ、ｊの両方もしくは片方を記録するようにして、実行装置１２は可搬媒体１１に記録されているパラメータｉ、ｊに従って検証するようにしてもよい。このパラメータｉ、ｊは、多くすればセキュリティは向上するが、処理時間が多くなり、少なくすれば処理時間は少なくなるが、セキュリティは低下するという特徴を有する。つまり、本変形例を用いることで、コンテンツ配布者のポリシーに依存して、セキュリティレベルなどを設定することが出来るようになる。なお、実行装置１２において、可搬媒体１１にパラメータｉ、ｊが記録されていない場合、予め与えられるデフォルトのパラメータｉ、ｊを用いるようにしても良い。
【０１３９】
（１８）実施の形態１において、可搬媒体１１には、さらに、不正なコンテンツかどうか検証するための情報を持たないコンテンツも同時に記録するようにしても良い。例えば、そのコンテンツの例としては、著作権保護等のセキュリティ技術の比較的必要のない映画のオープニング画面やＤＶＤのメニュー画面などである。そして、実施形態１で説明した実行装置１２による検証処理が終わるまで、それらコンテンツを実行するようにしても良い。それらコンテンツの例としては、違法コピーに関する警告文書、コンテンツ配給者のロゴやオープニング画面、ＤＶＤのメニュー画面などが挙げられる。なお、不正なコンテンツかどうか検証するための情報を持たないコンテンツは、予め実行装置１２内に格納されていても良い。それらコンテンツの例としては、実行装置１２が実行、再生可能なフォーマットのロゴや、実行装置１２の製造メーカのロゴなどが挙げられる。
【０１４０】
（１９）実施の形態１において、暗号化部分コンテンツの属性値（ハッシュ値）の集合を第一ハッシュテーブルとして、全ての第一ハッシュテーブルに対する属性値（ハッシュ値）を第二ハッシュテーブルとして、認証情報ＡＵＴＨはその第二ハッシュテーブルに対する認証情報としていたが、これに限るものではない。例えば、暗号化部分コンテンツの属性値（ハッシュ値）の集合を第一ハッシュテーブルとして、第一ハッシュテーブルをグループ分けし、その各グループの第一ハッシュテーブルを連結した値に対する属性値（ハッシュ値）を第二ハッシュテーブルとして、全ての第二ハッシュ値を連結した値に対する属性値（ハッシュ値）を第三ハッシュテーブルとして、認証情報ＡＵＴＨはその第三ハッシュテーブルに対する認証情報としてもよい。この場合、ヘッダ情報ＨＥＡＤには、第一ハッシュテーブル及び第二ハッシュテーブル及び第三ハッシュテーブルを含めることになる。このようにすることによって、可搬媒体から取得しなくてはならないハッシュ値の数を少なくすることが出来、処理時間をさらに短くすることが出来る。なお、同様に、第四ハッシュテーブル以降を用いることも出来る。
【０１４１】
（２０）実施の形態１の可搬媒体１１において記録されているデータに加え、さらに、可搬媒体に部分コンテンツの実行手順を記述したデータである実行手順データＮＡＶを記録していており、実行装置１２の実行部１２９では、その実行手順データＮＡＶを基に、部分コンテンツを実行するような場合に、可搬媒体に、さらに、図２９で示すように、その実行手順データＮＡＶに対する認証情報として実行手順データ認証情報ＮＡＶＡＵＴＨを記録するようにして、認証情報検証部１２６では、その実行手順データ認証情報ＮＡＶＡＵＴＨが実行手順データＮＡＶに対する正規の認証情報である場合にのみ、実行部１２９へ暗号化コンテンツＥＮＣＣＮＴ及びコンテンツ鍵ＣＫを出力するようにしてもよい。ここで、実行手順データＮＡＶは、例えば、ＤＶＤ－ＶＩＤＥＯ形式におけるナビゲーションファイル（拡張子がＩＦＯのファイル）である。これにより、さらに強い不正コンテンツをも検知できる不正コンテンツ検知システムが実現出来る。
【０１４２】
（２１）実施の形態１において、可搬媒体１２に記録されるヘッダ情報ＨＥＡＤは、見

出し情報として、暗号化コンテンツＥＮＣＣＮＴの必ず前側についているとは限らない。例えば、ヘッダ情報ＨＥＡＤではなく、付加情報や検証対象データとして、暗号化コンテンツＥＮＣＣＮＴの後ろ側（フッタ）についていても構わない。

【０１４３】

（２２）実施の形態１において、コンテンツＣＮＴが予めｎ個に分割されていない場合であっても、暗号化部１０５はある所定の規則に従ってコンテンツＣＮＴをｎ個に分割するようにしても良い。この場合、所定の規則は、例えば、外部から入力されるようにしてもよい。これは、例えば、暗号化部１０５がキーボードやマウスと接続されていることにより実現できる。また、所定の規則は、システム共通のパラメータとして与えられていても良い。ここでのある所定の規則とは、例えば、６４キロバイト単位、１メガバイト単位、１秒単位、１分単位、１秒単位といった情報である。また、別の例として、コンテンツデータがＤＶＤ－ＶＩＤＥＯ形式の動画コンテンツの場合、例えば、ＶＯＢ単位や、ＶＯＢＵ（Ｖｉｄｅｏ　ＯＢｊｅｃｔＵｎｉｔ）単位、セル（Ｃｅｌｌ）単位などである。コンテンツデータがＭＰＥＧ２形式の動画コンテンツの場合、例えば、ＧＯＰ単位、フィールド単位、フレーム単位、Ｉピクチャ単位などである。コンテンツデータがディスクに記録されている場合、例えば、セクタ単位、論理セクタ単位、トラック単位、シリンダ単位、ブロック単位、エラー訂正に使用する拘束長（ＥＣＣブロック単位）などである。なお、それぞれの部分コンテンツの分割単位（サイズなど）は、全て同じである必要はなく、それぞれ異なっていても良い。また、コンテンツを分割する数（ｎ）は、コンテンツＣＮＴに応じて変えても良い。また、コンテンツを分割する単位は、また、可搬媒体１１に記録されているようにしてもよい。

【０１４４】

（２３）実施の形態１において、コンテンツ位置情報ＰＯＳは、図９のような構成であったが、これに限るものではなく、暗号化部分コンテンツの構成を、及び、暗号化部分コンテンツの中のユニットの構成を特定出来るものであれば、どのようなものでもよい。例えば、特定情報は、暗号化部分コンテンツを識別する光ディスク上の先頭の物理アドレスとデータサイズや、先頭の物理アドレスと終端の物理アドレスであっても良い。さらに、ユニット数の替わりに、各ユニットの先頭の論理アドレスとデータサイズの羅列、もしくは、先頭と終端の論理アドレスの羅列、もしくは、先頭の物理アドレスとデータサイズの羅列、もしくは、先頭と終端の物理アドレスの羅列であっても良い。

【０１４５】

また、コンテンツ位置情報ＰＯＳにおいて、各特定情報に対応する暗号化部分コンテンツに含まれるユニット数が同じ場合、図３０で示すとおり、ｎ個のユニット数の替わりに１つの共通ユニット数ＡＬＬＮＵＭＵ（一つの第二ハッシュ値が、いくつの第一ハッシュ値から計算されているかを示す属性値比率）がコンテンツ位置情報ＰＯＳに含まれていても良い。この場合、認証情報ＡＵＴＨは、図３１で示すように、第二ハッシュテーブルＨＡＳＨＴＢＬ２及び共通ユニット数ＡＬＬＮＵＭＵを連結した値に対する認証情報であっても良く、実行装置１２における検証時には、認証情報ＡＵＴＨが入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２及び共通ユニット数ＡＬＬＮＵＭＵを連結した値に対する正しい認証情報であるか検証するようにしても良い。

【０１４６】

（２４）本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしても良い。また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、リムーバブルディスク、ハードディスク、ＣＤ、ＭＯ、ＤＶＤ、ＳＤメモリカード、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とする通信ネットワーク等を経由して伝送するものとしても

よい。また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記通信ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

【０１４７】

（２５）上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【産業上の利用可能性】

【０１４８】

本発明にかかる不正コンテンツ検知システムは、実行装置においてコンテンツを実行開始、もしくは再生開始する前に、そのコンテンツが想定する主体（例えば正規の著作権を有する人・団体・会社）により配布されたコンテンツかどうかを検知できるという機能を有し、その検知結果によりコンテンツの実行開始、再生開始を制御（例えば警告、停止、禁止）することが出来る。これは、コンテンツの著作権保護が必要とされるシステム全般、特に記録媒体や可搬媒体（例えば光ディスクやメモリカード）や通信ネットワーク、放送網を用いたコンテンツ配布システムに有用である。

【０１４９】

さらに、本発明は、動画データや音声データなどのマルチメディアコンテンツに限らず、コンテンツの実行順序を制御する実行順序ファイル（ナビゲーションファイル）や、コンピュータプログラム等の保護にも適用可能である。この場合、実行装置において、不正なコンピュータプログラム（例えばコンピュータウイルスを含むコンピュータプログラム）を実行開始しない等が実現出来る。そのため、安全（セキュア）な処理環境を実現するコンピュータシステム全般、特にＯＳ（Ｏｐｅｒａｔｉｏｎ　Ｓｙｓｔｅｍ）等としても有用である。

【図面の簡単な説明】

【０１５０】

【図１】本発明の実施の形態１における不正コンテンツ検知システムの概要図

【図２】本発明の実施の形態１における配布センタ１０の構成例を示す図

【図３】本発明の実施の形態１における実行装置情報格納部１０３の構成例を示す図

【図４】本発明の実施の形態１における暗号化鍵束ＫＢの一例を示す図

【図５】本発明の実施の形態１における暗号化コンテンツＥＮＣＣＮＴの作成方法の一例を示す図

【図６】本発明の実施の形態１におけるヘッダ情報ＨＥＡＤの作成方法の一例を示す図

【図７】本発明の実施の形態１における第一ハッシュテーブルＨＡＳＨＴＢＬ１＃１の作成方法の一例を示す図

【図８】本発明の実施の形態１における第二ハッシュテーブルＨＡＳＨＴＢＬ２の作成方法の一例を示す図

【図９】本発明の実施の形態１におけるコンテンツ位置情報ＰＯＳの一例を示す図

【図１０】本発明の実施の形態１における認証情報ＡＵＴＨの作成方法の一例を示す図

【図１１】本発明の実施の形態１における配布センタ１０の処理の流れ図（一例）

【図１２】本発明の実施の形態１における可搬媒体１１に記録されるデータの一例を示す図

【図１３】本発明の実施の形態１における実行装置１２の構成例を示す図

【図１４】本発明の実施の形態１におけるコンテンツ位置情報ＰＯＳからｉ組の特定情報とユニット数を選択する場合の一例を示す図

【図１５】本発明の実施の形態１における入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２の作成方法の一例を示す図

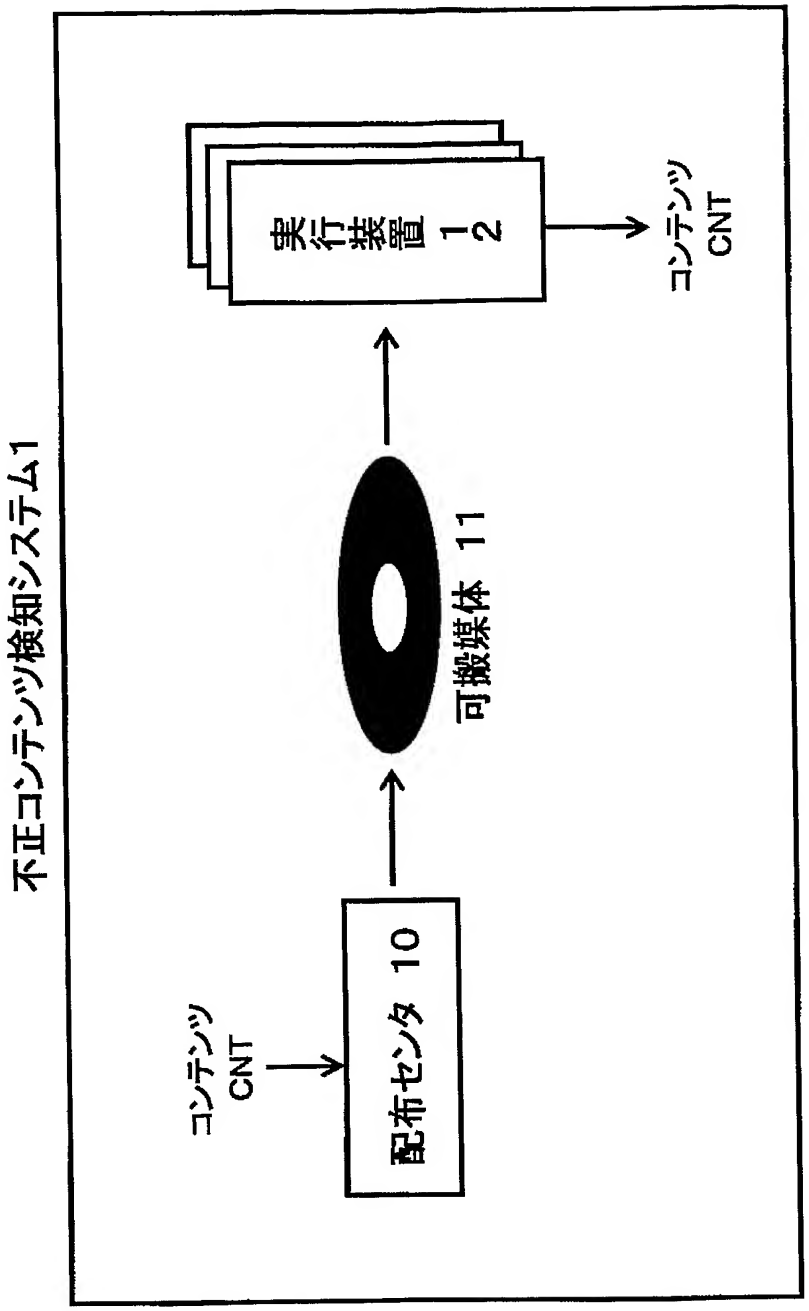
【図１６】本発明の実施の形態１における入替第一ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ１＃１の作成方法の一例を示す図
【図１７】本発明の実施の形態１における入替第二ハッシュテーブルＲＥＰＨＡＳＨＴＢＬ２の作成方法の一例を示す図
【図１８】本発明の実施の形態１における認証情報ＡＵＴＨの検証方法の一例を示す図
【図１９】実行装置１２の処理の一例を示す流れ図
【図２０】認証情報生成情報格納部１０７の別の一例を示す図
【図２１】検証情報格納部１２５の別の一例を示す図
【図２２】認証情報生成情報格納部１０７の別の一例を示す図
【図２３】検証情報格納部１２５の別の一例を示す図
【図２４】認証情報ＡＵＴＨの別の検証方法の一例（ステップ１）を示す図
【図２５】認証情報ＡＵＴＨの別の検証方法の一例（ステップ２）を示す図
【図２６】認証情報ＡＵＴＨの別の検証方法の一例（ステップ２の詳細１）を示す図
【図２７】認証情報ＡＵＴＨの別の検証方法の一例（ステップ２の詳細２）を示す図
【図２８】可搬媒体１２（光ディスク）と取得部１２１の一例を示す図
【図２９】可搬媒体１１に記録されるデータの別の一例を示す図
【図３０】コンテンツ位置情報ＰＯＳの別の一例を示す図
【図３１】認証情報ＡＵＴＨの作成方法の別の一例を示す図
【図３２】認証情報ＡＵＴＨの検証方法の別の一例を示す図
【図３３】従来技術の可搬媒体に記録されるデータの構成を示す図

【符号の説明】

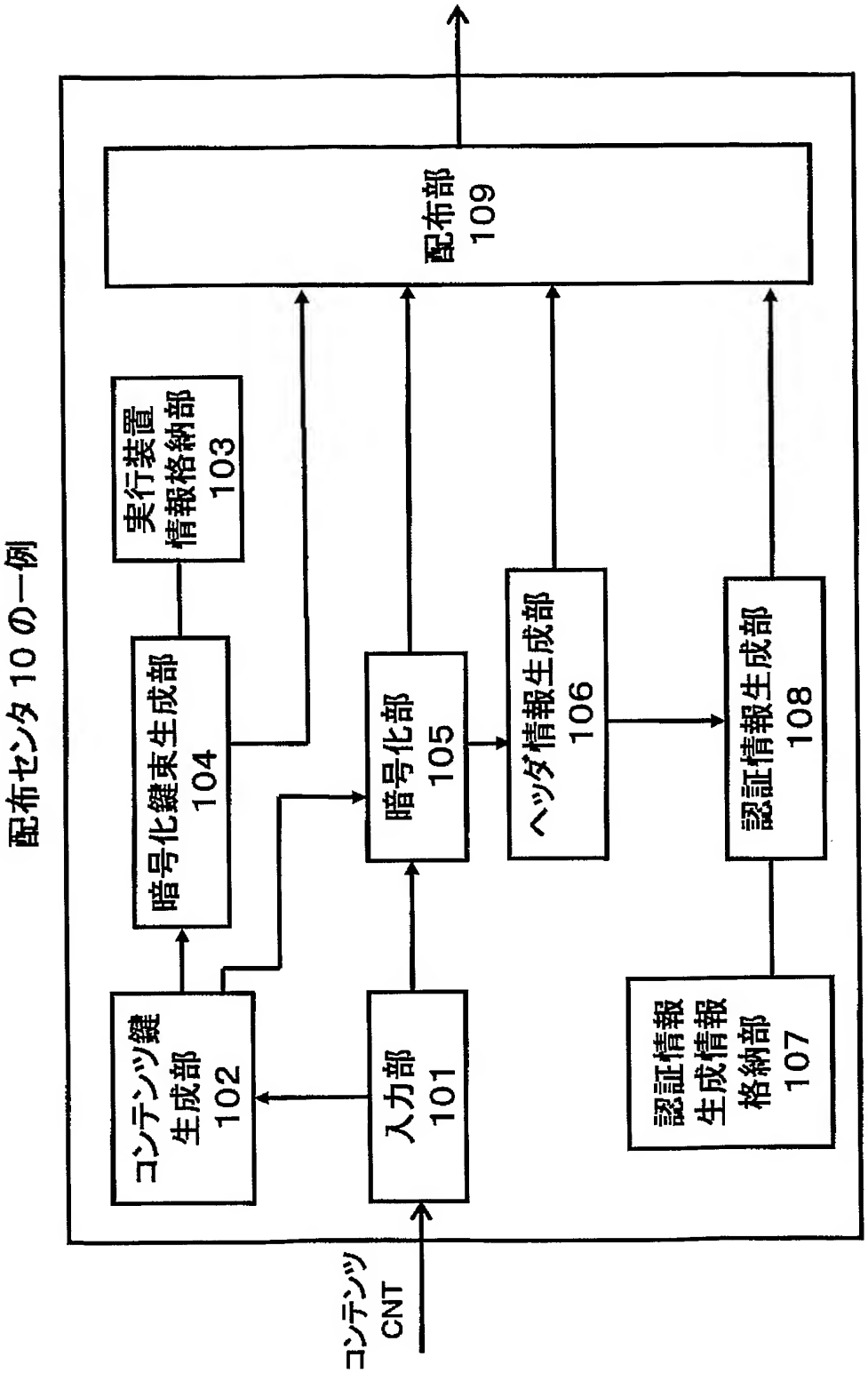
【０１５１】

１０　配布センタ
１１　可搬媒体
１２　実行装置
１０１　入力部
１０２　コンテンツ鍵生成部
１０３　実行装置情報格納部
１０４　暗号化鍵束生成部
１０５　暗号化部
１０６　ヘッダ情報生成部
１０７　認証情報生成情報格納部
１０８　認証情報生成部
１０９　配布部
１２１　取得部
１２２　デバイス鍵格納部
１２３　コンテンツ鍵取得部
１２４　検証情報格納部
１２５　認証情報検証部
１２６　実行部

【書類名】図面
【図１】

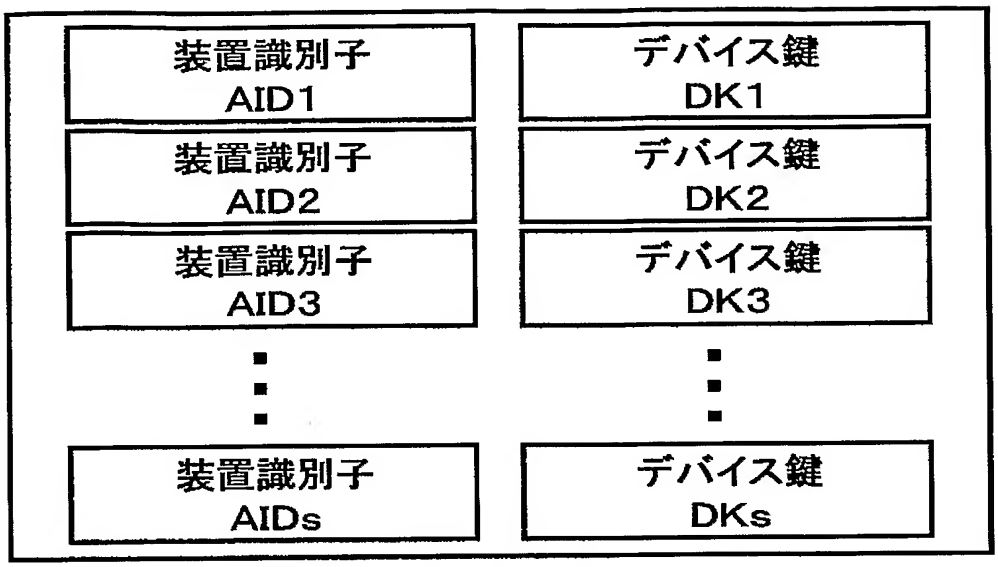


【図２】


配布センタ１０の一例
配布部
109
実行装置
情報格納部
103
暗号化鍵束生成部
104
暗号化部
105
ヘッダ情報生成部
106
認証情報生成部
108
コンテンツ鍵
生成部
102
入力部
101
認証情報
生成情報
格納部
107
コンテンツ
CNT

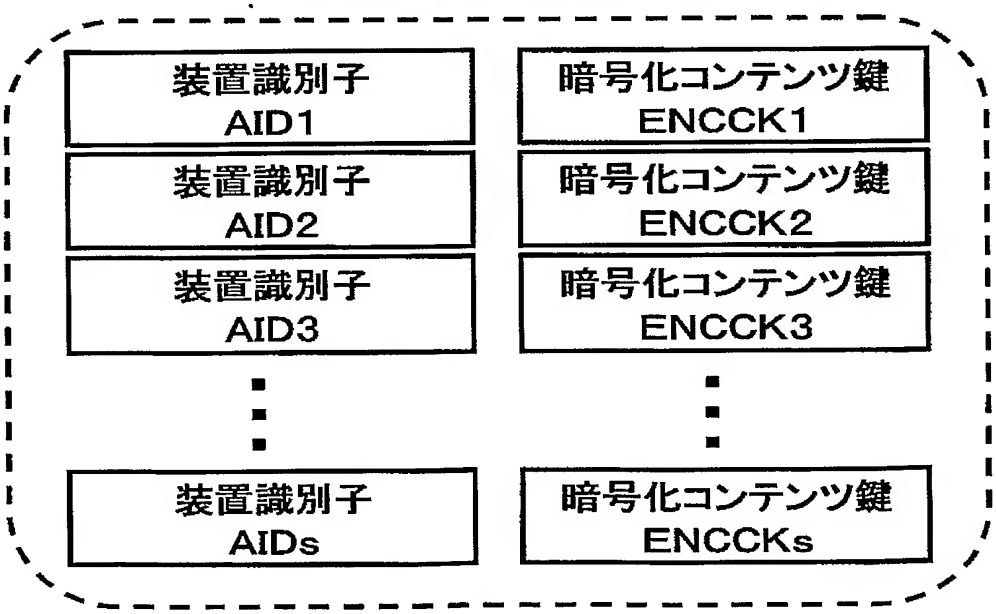
【図３】

実行装置情報格納部103の一例



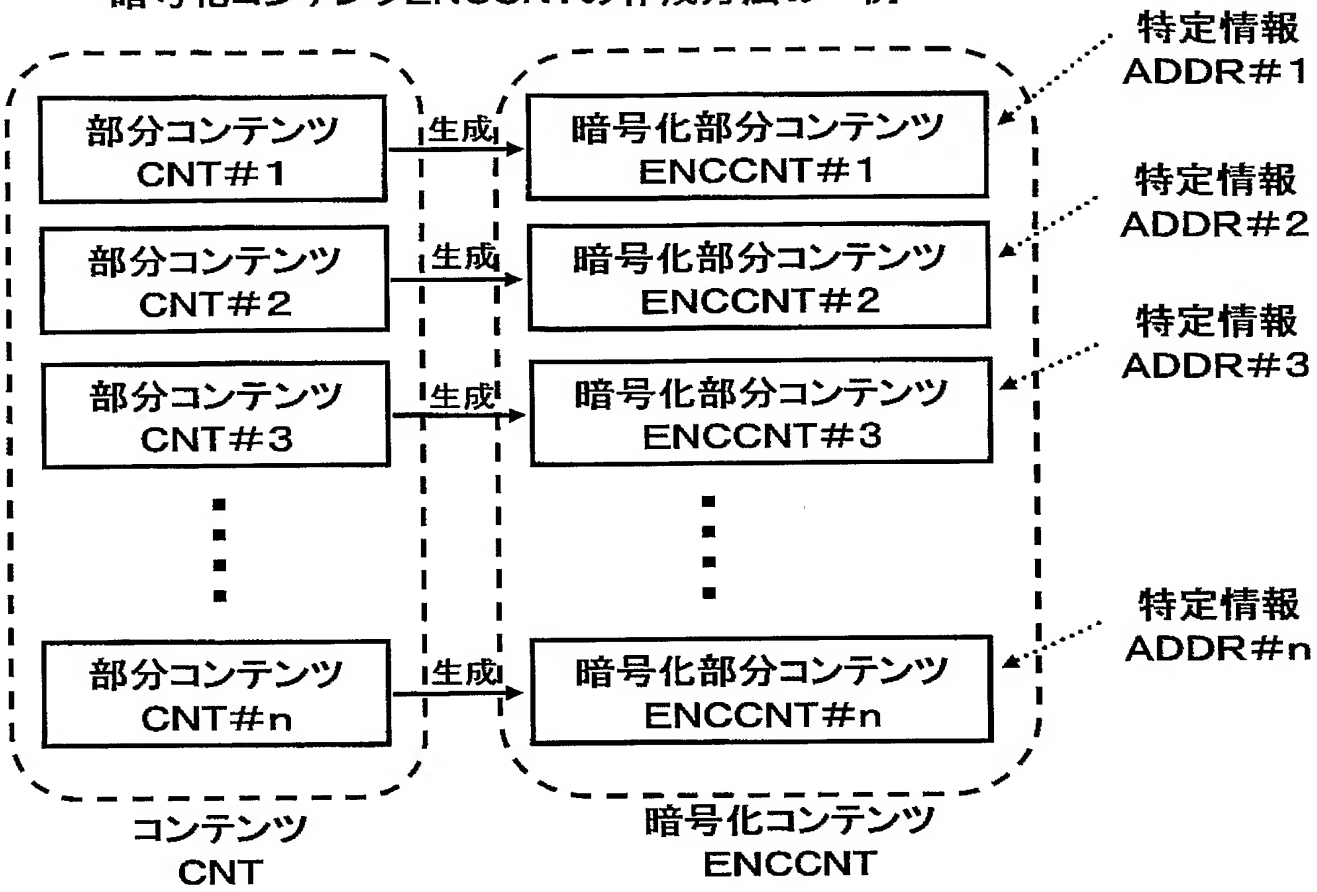
【図４】

暗号化鍵束　KBの一例

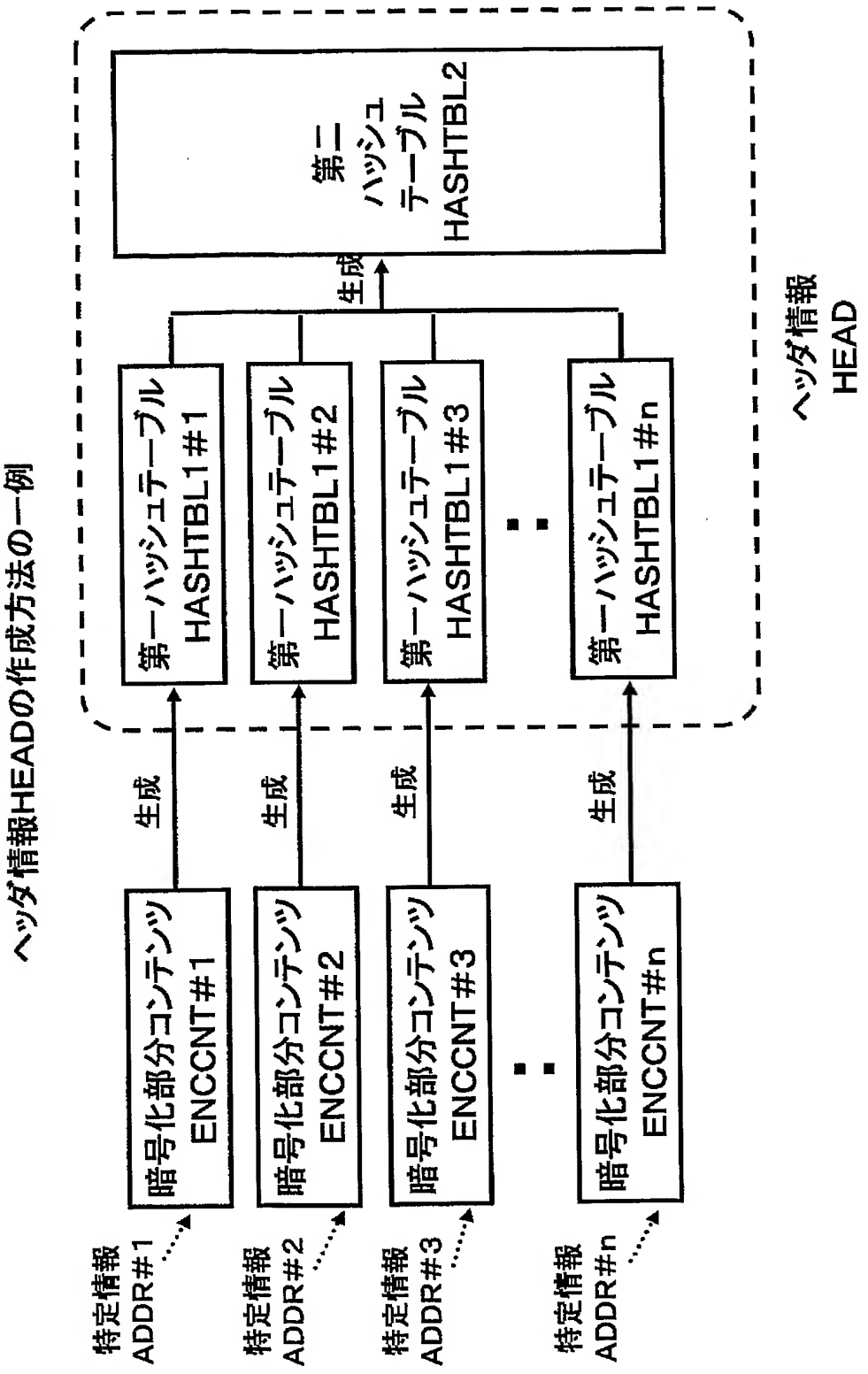


【図５】

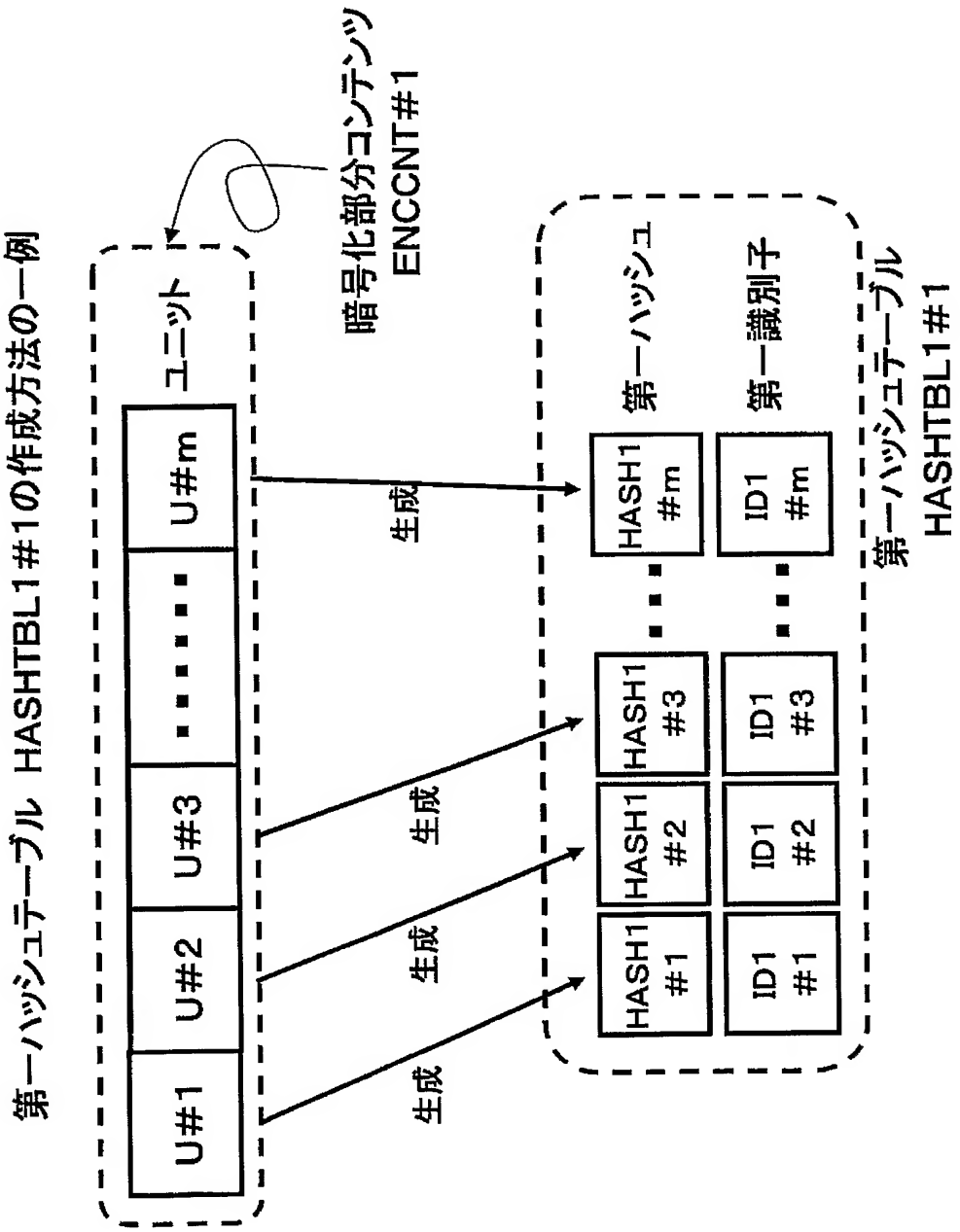
暗号化コンテンツENCCNTの作成方法の一例



【図６】

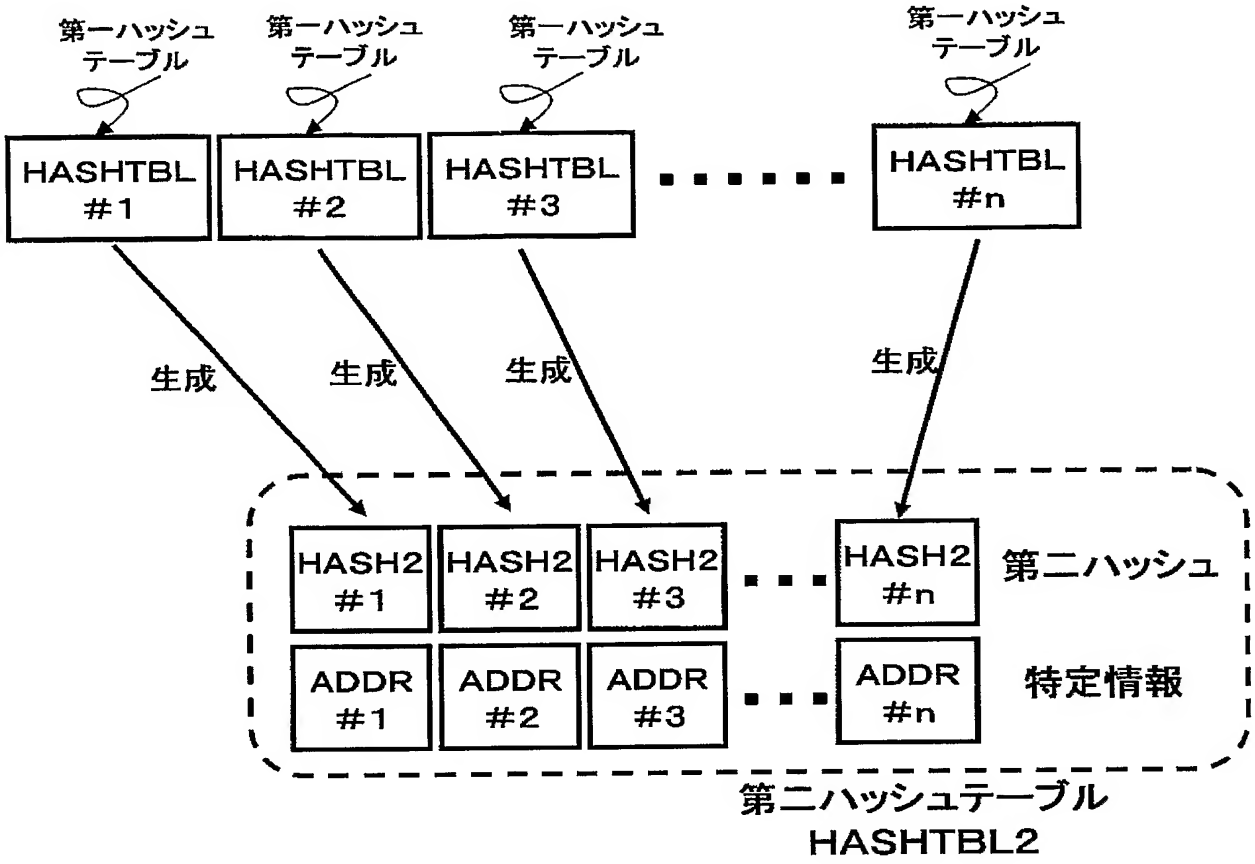

ヘッダ情報HEADの作成方法の一例
ヘッダ情報
HEAD
第二
ハッシュ
テーブル
HASHTBL2
生成
第一ハッシュテーブル
HASHTBL1#1
第一ハッシュテーブル
HASHTBL1#2
第一ハッシュテーブル
HASHTBL1#3
第一ハッシュテーブル
HASHTBL1#n
生成
生成
生成
生成
暗号化部分コンテンツ
ENCCNT#1
暗号化部分コンテンツ
ENCCNT#2
暗号化部分コンテンツ
ENCCNT#3
暗号化部分コンテンツ
ENCCNT#n
特定情報
ADDR#1
特定情報
ADDR#2
特定情報
ADDR#3
特定情報
ADDR#n

【図７】


第一ハッシュテーブル HASHTBL1#1の作成方法の一例
ユニット
U#1
U#2
U#3
U#m
暗号化部分コンテンツ
ENCCNT#1
生成
生成
生成
生成
第一ハッシュ
第一識別子
HASH1 #1
HASH1 #2
HASH1 #3
HASH1 #m
ID1 #1
ID1 #2
ID1 #3
ID1 #m
第一ハッシュテーブル
HASHTBL1#1

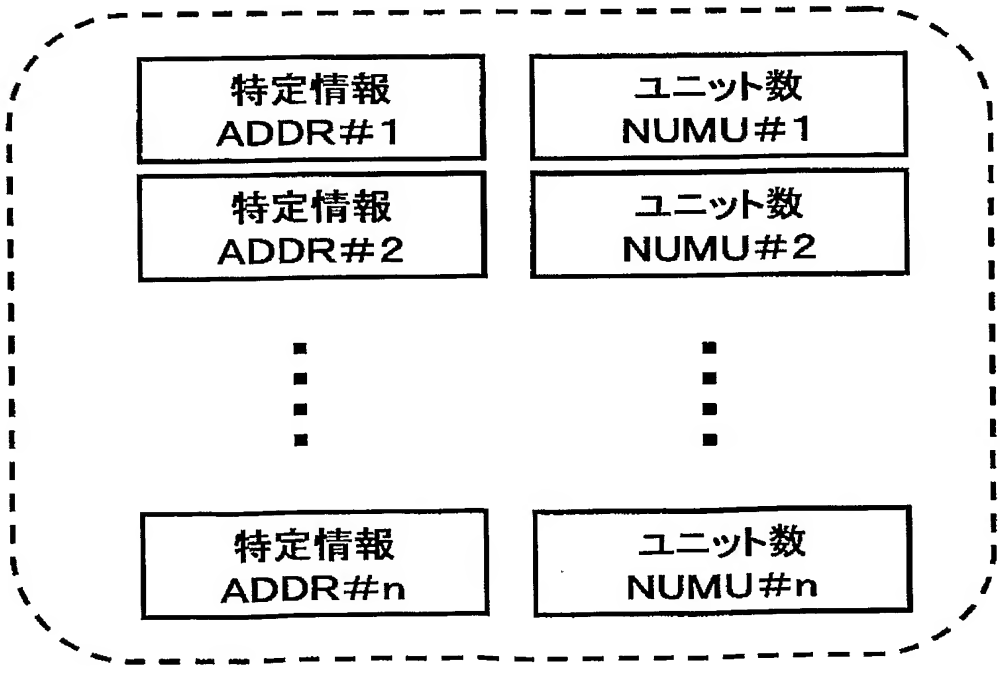
【図８】

第二ハッシュテーブル　HASHTBL2の作成方法の一例



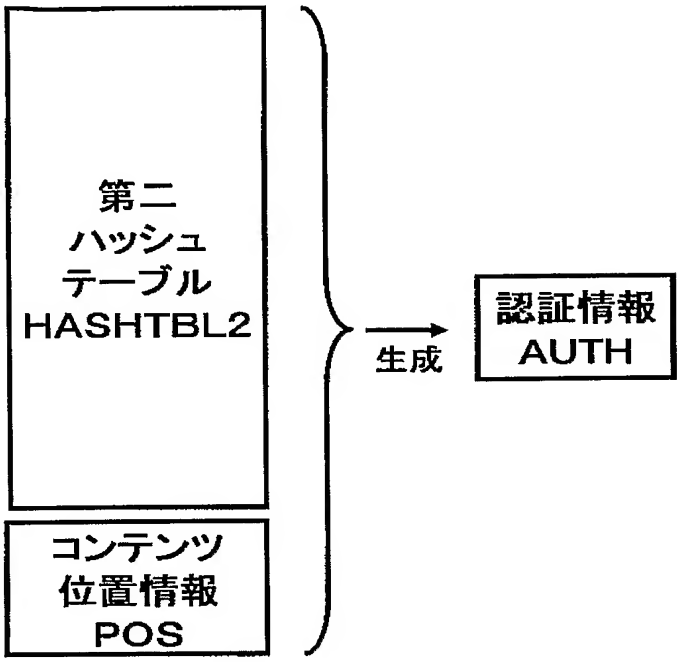
【図９】

コンテンツ位置情報　POSの一例

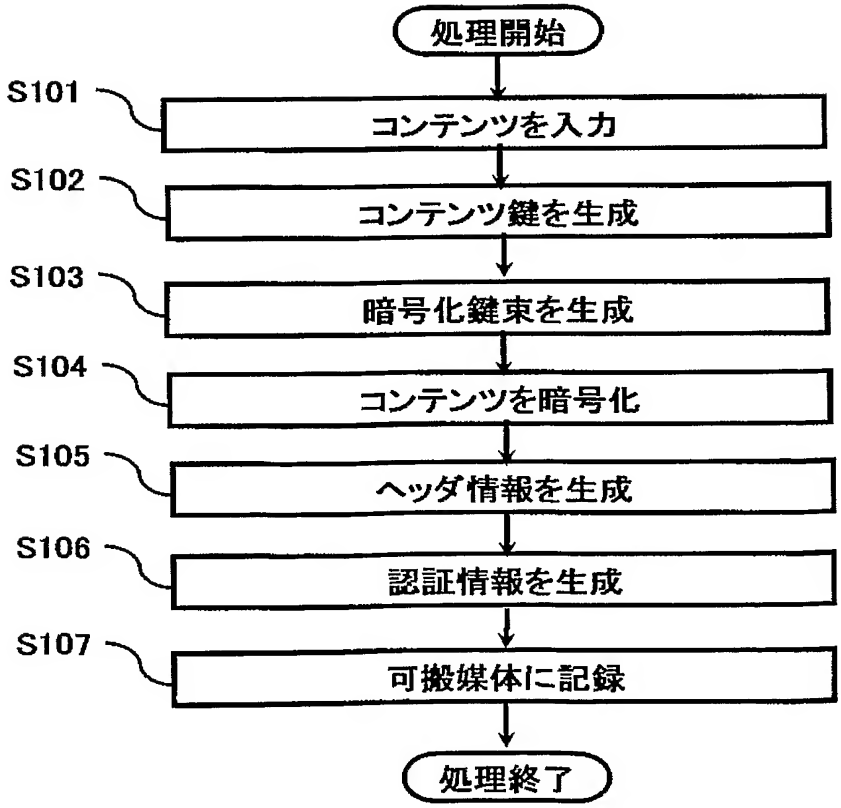


【図１０】

認証情報AUTHの作成方法の一例

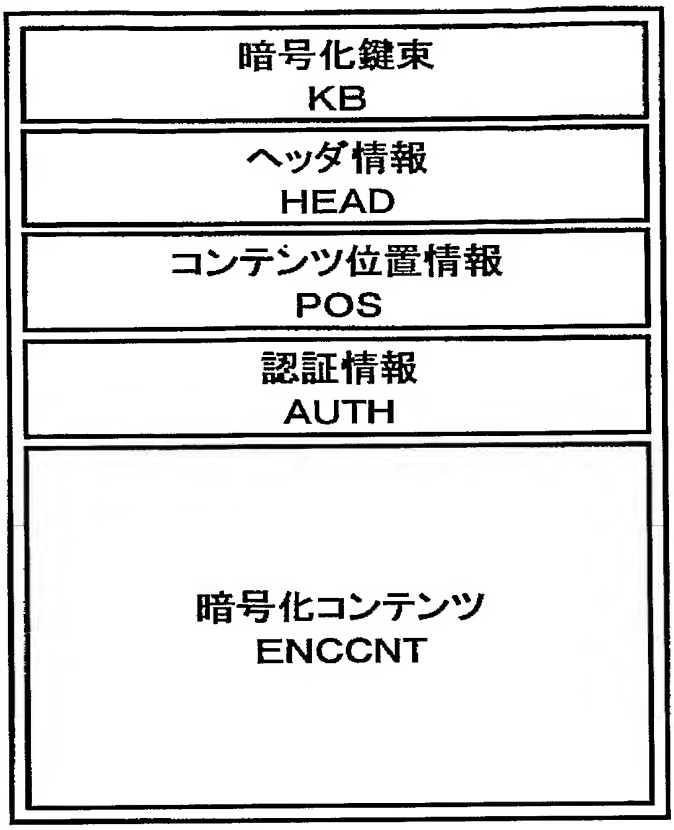


【図１１】

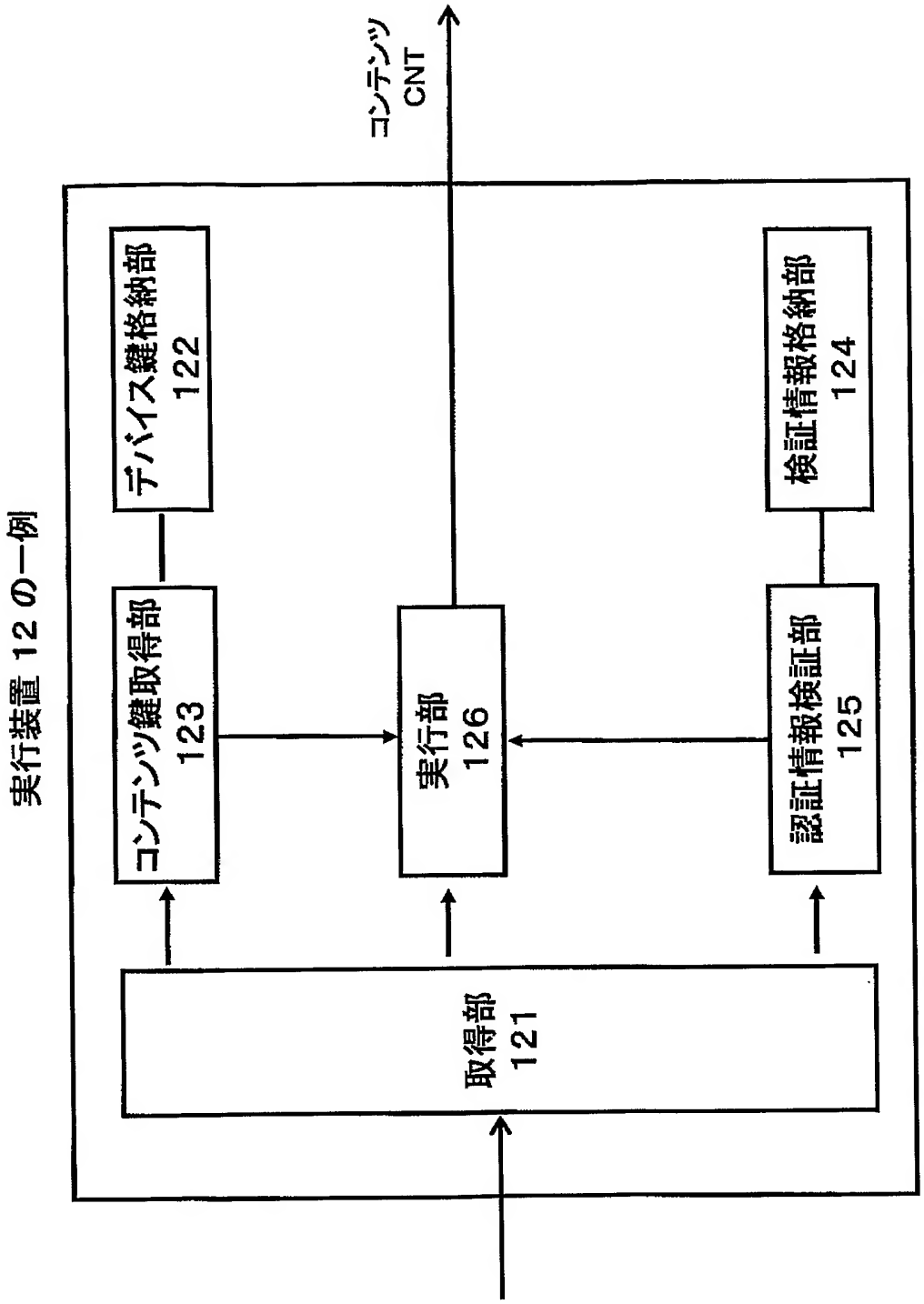


【図１２】

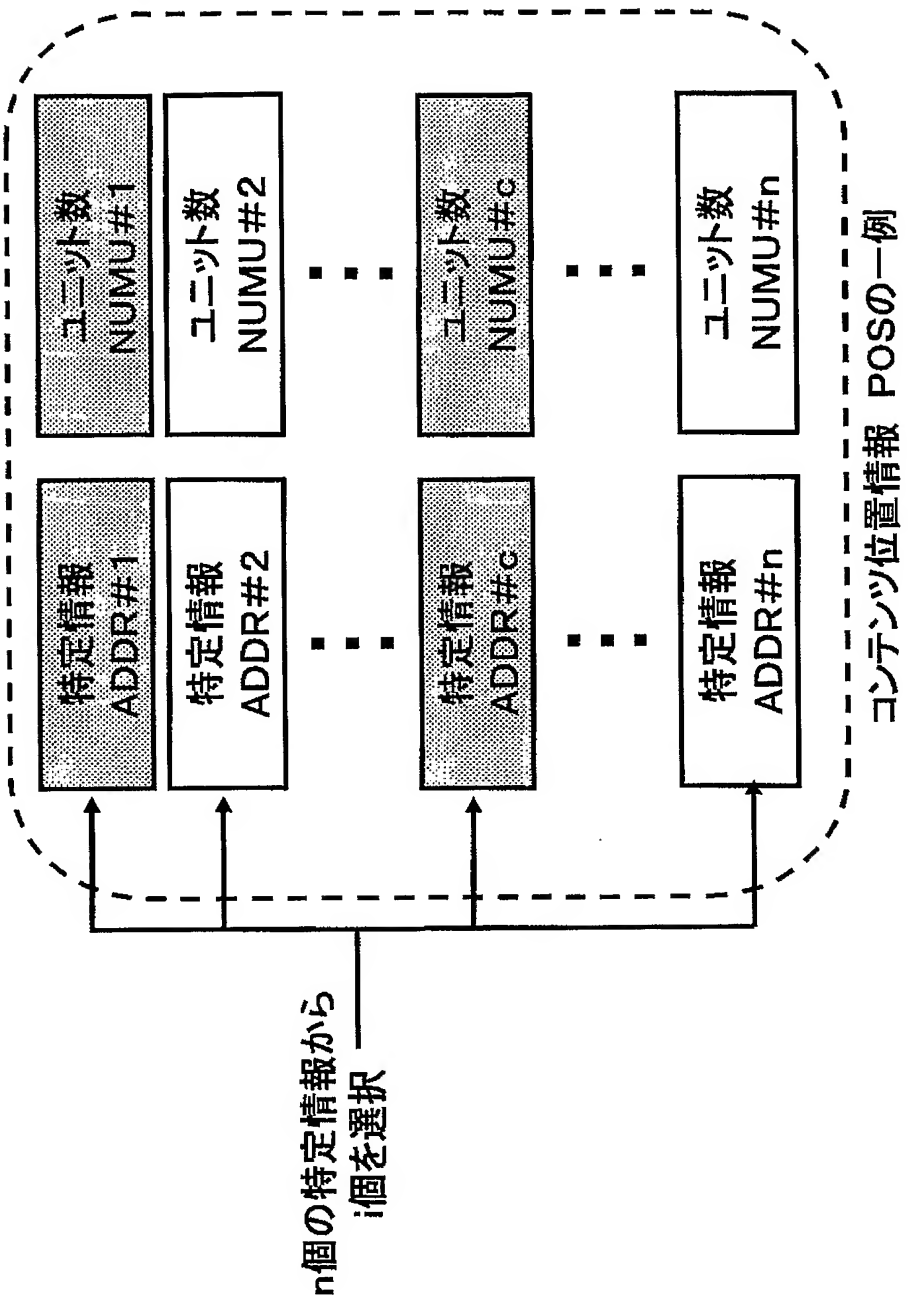
可搬媒体１１に記録されるデータの一例



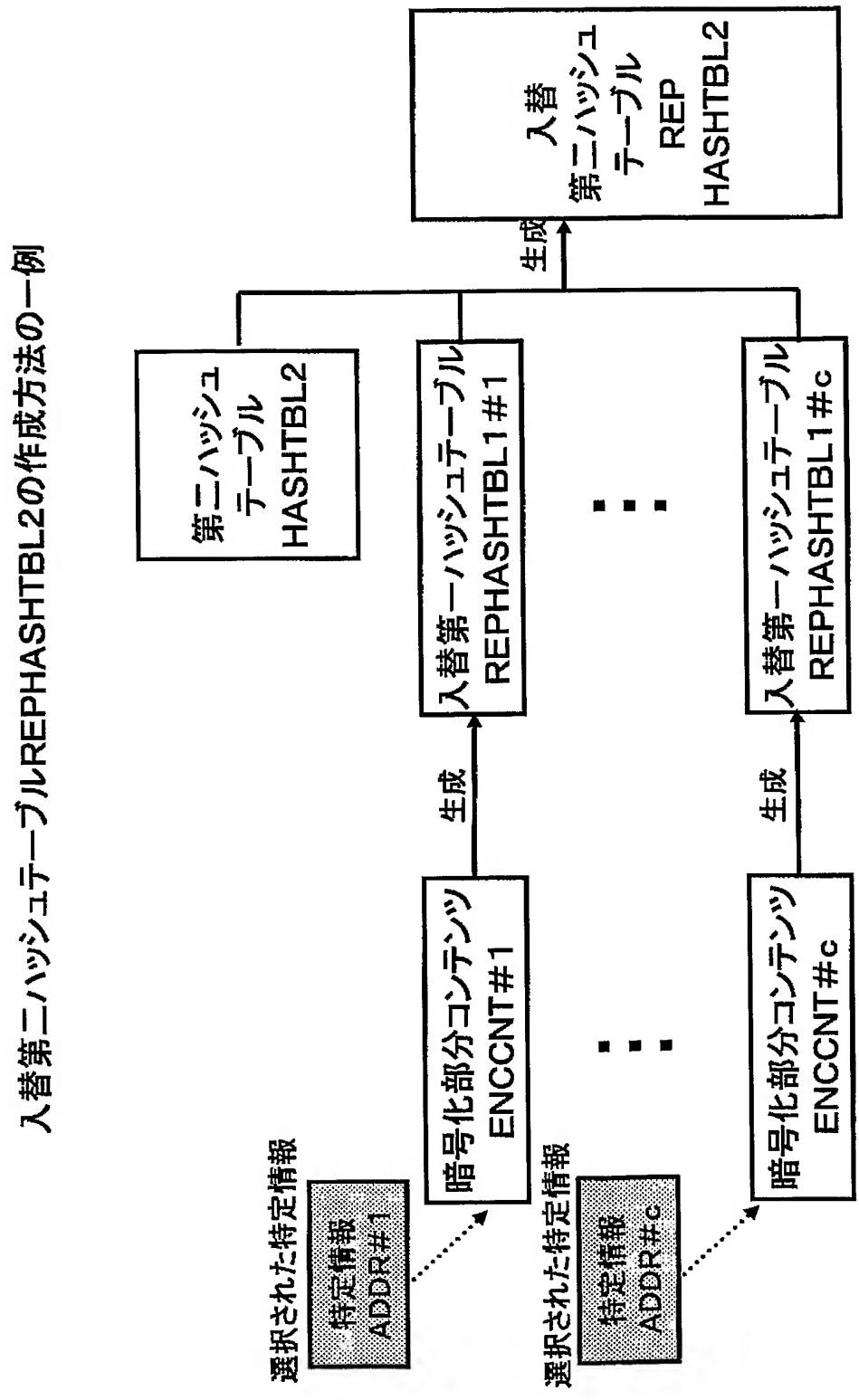
【図１３】


実行装置 12 の一例
コンテンツ
CNT
デバイス鍵格納部
122
検証情報格納部
124
コンテンツ鍵取得部
123
実行部
126
認証情報検証部
125
取得部
121

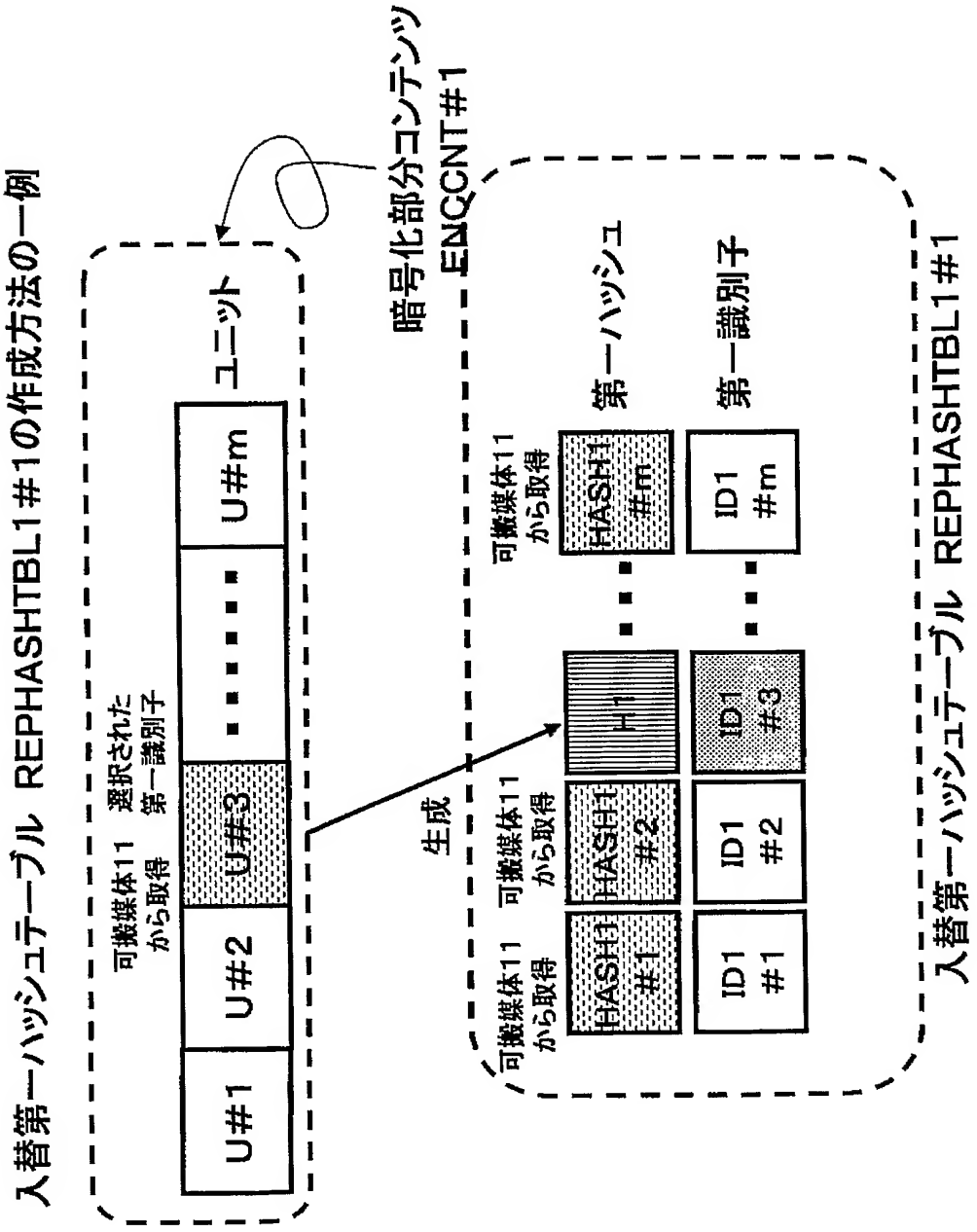
【図１４】


ユニット数
NUMU#1
ユニット数
NUMU#2
ユニット数
NUMU#c
ユニット数
NUMU#n
特定情報
ADDR#1
特定情報
ADDR#2
特定情報
ADDR#c
特定情報
ADDR#n
コンテンツ位置情報 POSの一例
n個の特定情報から
i個を選択

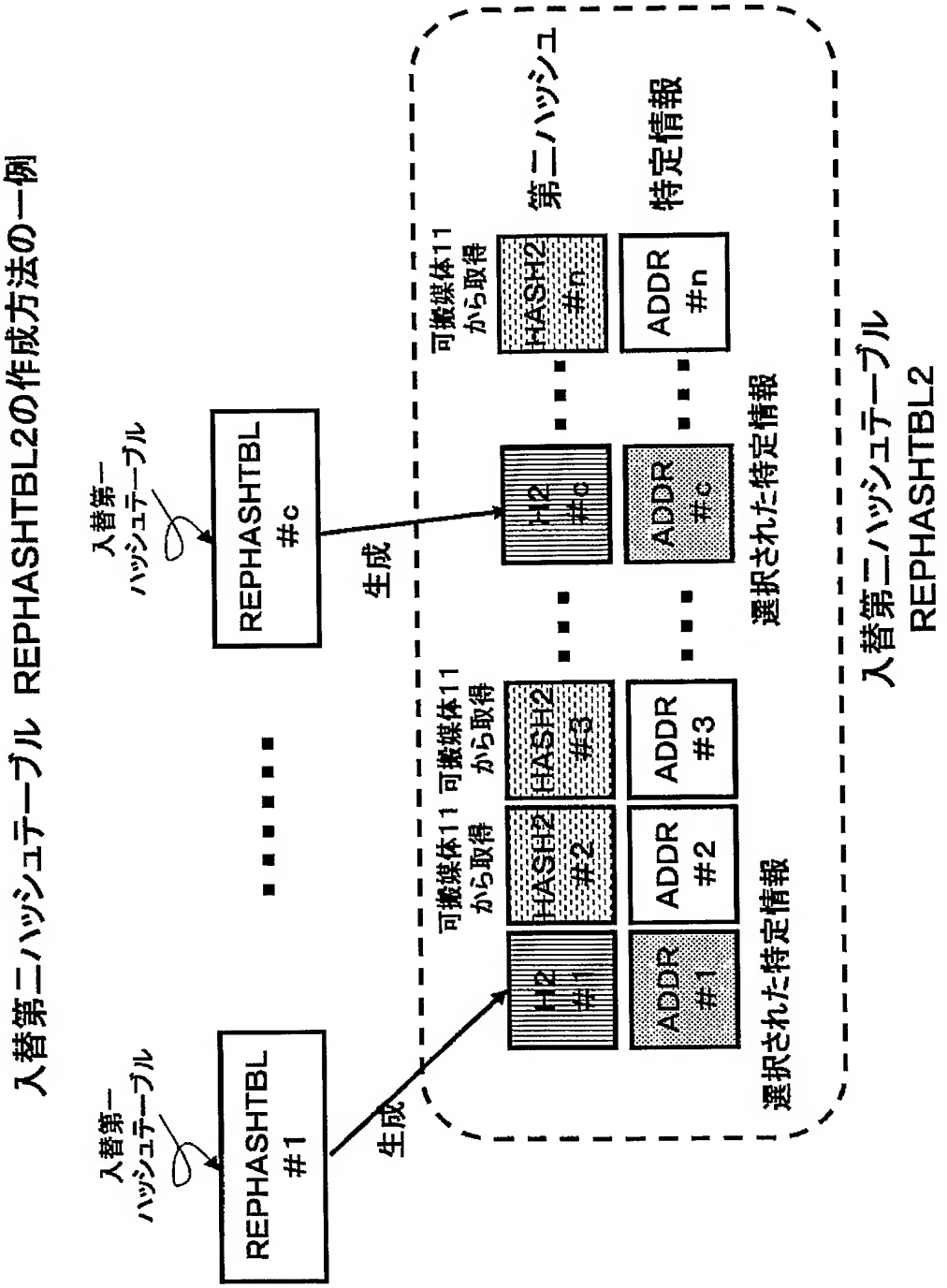
【図１５】


入替第二ハッシュテーブルREPHASHTBL2の作成方法の一例
第二ハッシュテーブル HASHTBL2
生成
入替第二ハッシュテーブル REP HASHTBL2
入替第一ハッシュテーブル REPHASHTBL1#1
入替第一ハッシュテーブル REPHASHTBL1#c
生成
生成
暗号化部分コンテンツ ENCCNT#1
暗号化部分コンテンツ ENCCNT#c
選択された特定情報
特定情報 ADDR#1
選択された特定情報
特定情報 ADDR#c

【図１６】

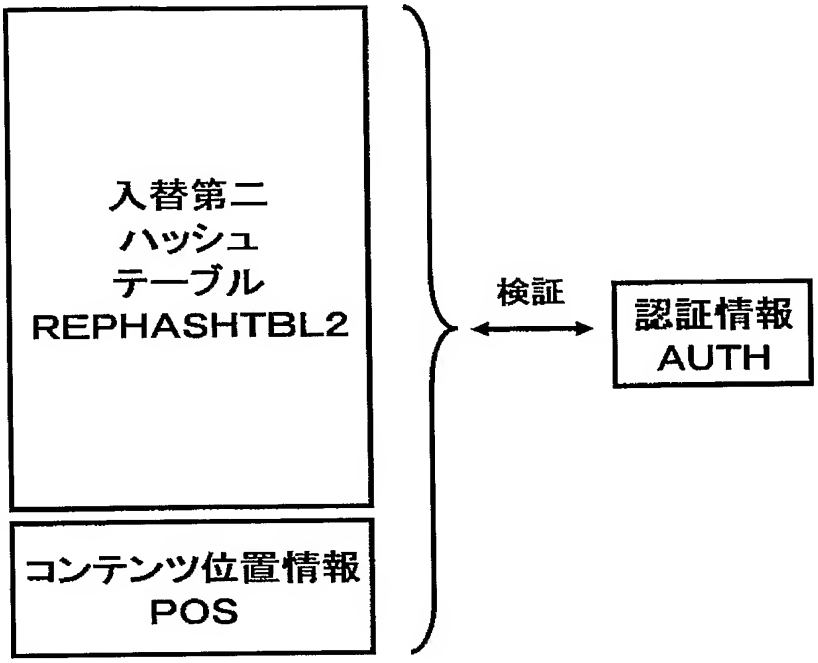

入替第一ハッシュテーブル REPHASHTBL1#1の作成方法の一例
暗号化部分コンテンツ
ENCCNT#1
ユニット
U#1
U#2
U#3
U#m
可搬媒体11
から取得
選択された
第一識別子
生成
可搬媒体11
から取得
可搬媒体11
から取得
第一ハッシュ
第一識別子
HASH1
#1
HASH1
#2
H1
HASH1
#m
ID1
#1
ID1
#2
ID1
#3
ID1
#m
入替第一ハッシュテーブル REPHASHTBL1#1

【図１７】

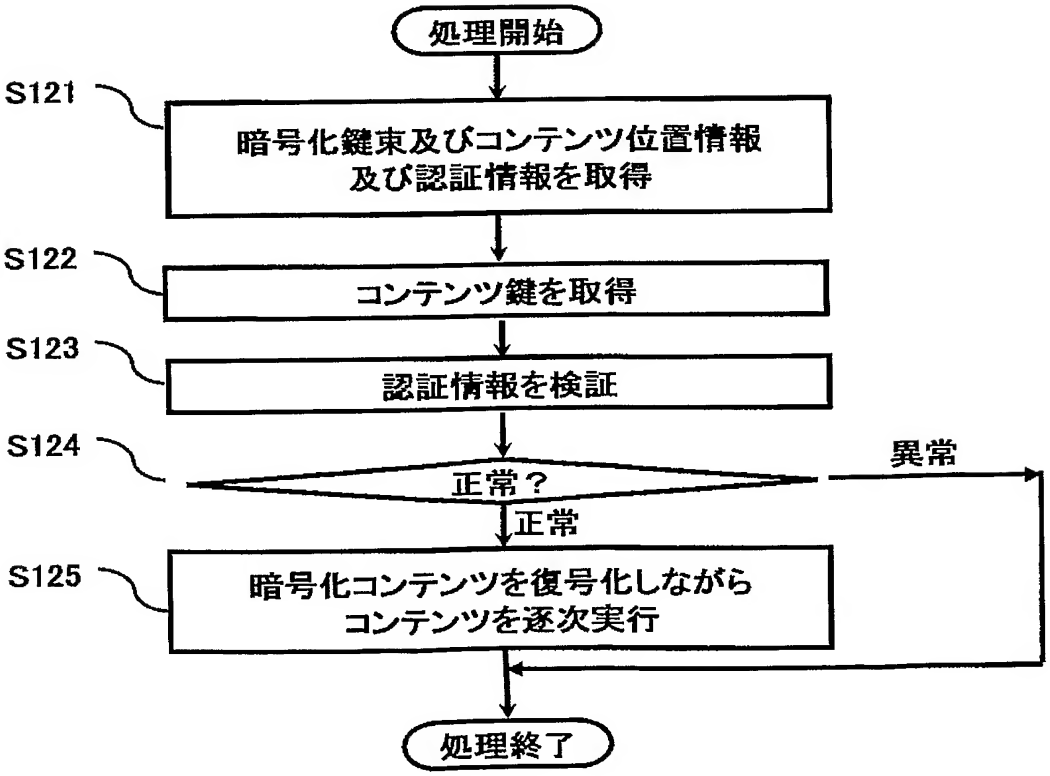

入替第二ハッシュテーブル REPHASHTBL2の作成方法の一例
入替第一ハッシュテーブル
REPHASHTBL #1
入替第一ハッシュテーブル
REPHASHTBL #c
生成
生成
可搬媒体11から取得
可搬媒体11から取得
H2 #1
HASH2 #2
HASH2 #3
H2 #c
HASH2 #n
ADDR #1
ADDR #2
ADDR #3
ADDR #c
ADDR #n
第二ハッシュ
特定情報
選択された特定情報
選択された特定情報
入替第二ハッシュテーブル
REPHASHTBL2

【図１８】

認証情報AUTHの検証方法の一例

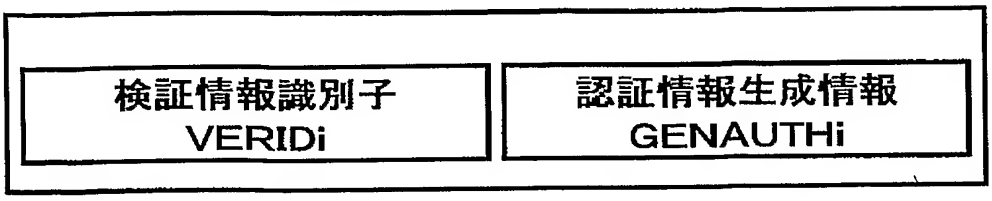


【図１９】



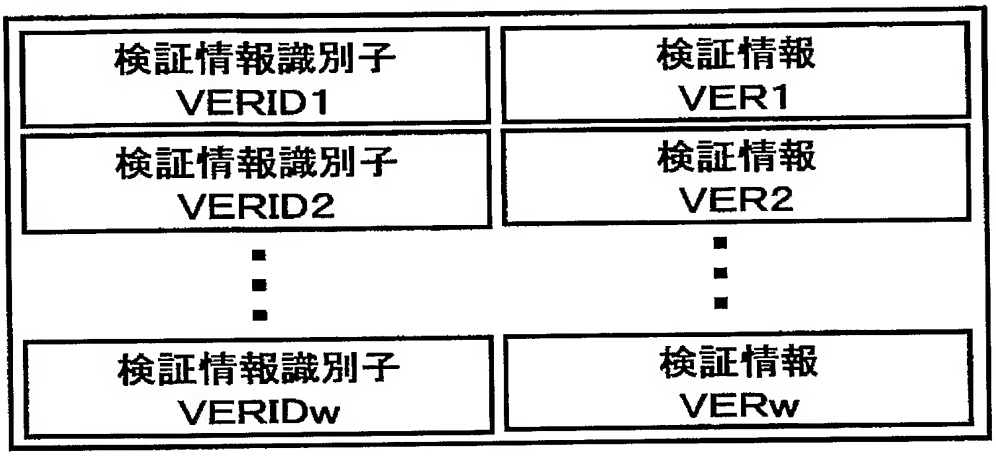
【図２０】

認証情報生成情報格納部107の別の一例



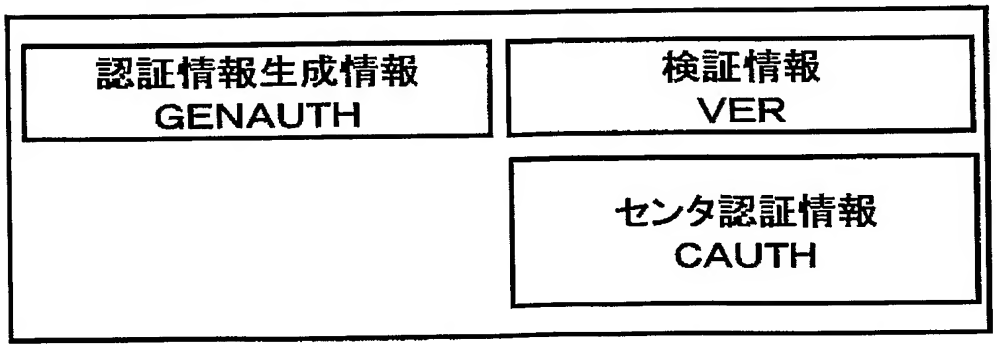
【図２１】

検証情報格納部125の別の一例



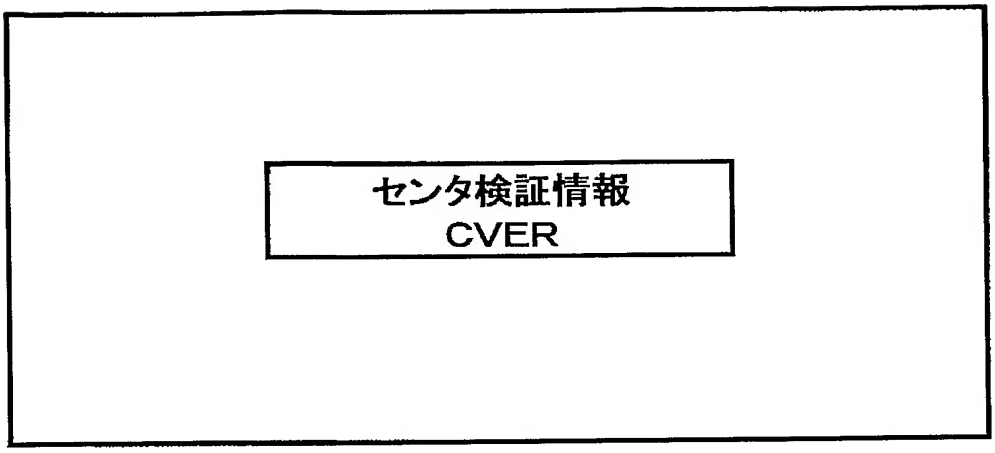
【図２２】

認証情報生成情報格納部107の別の一例



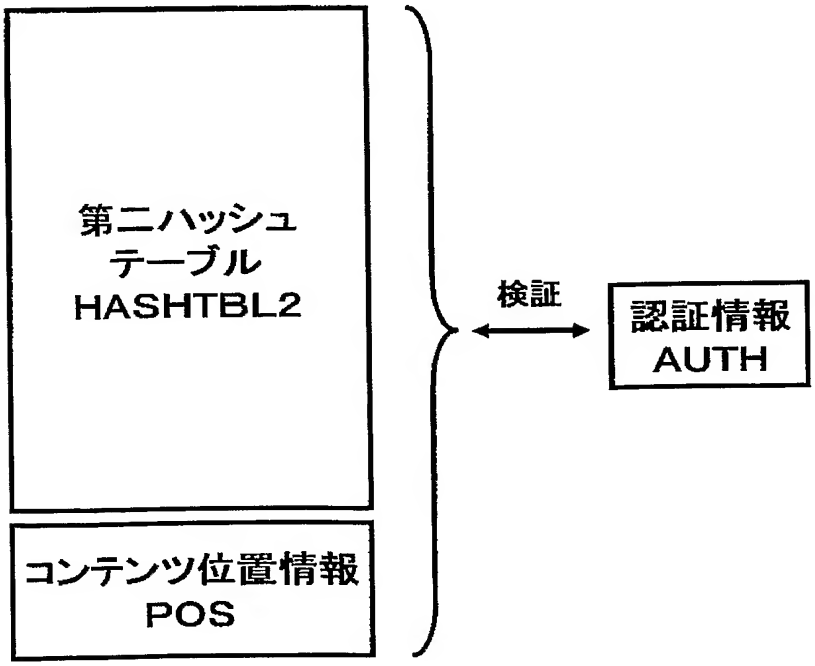
【図２３】

検証情報格納部125の別の一例



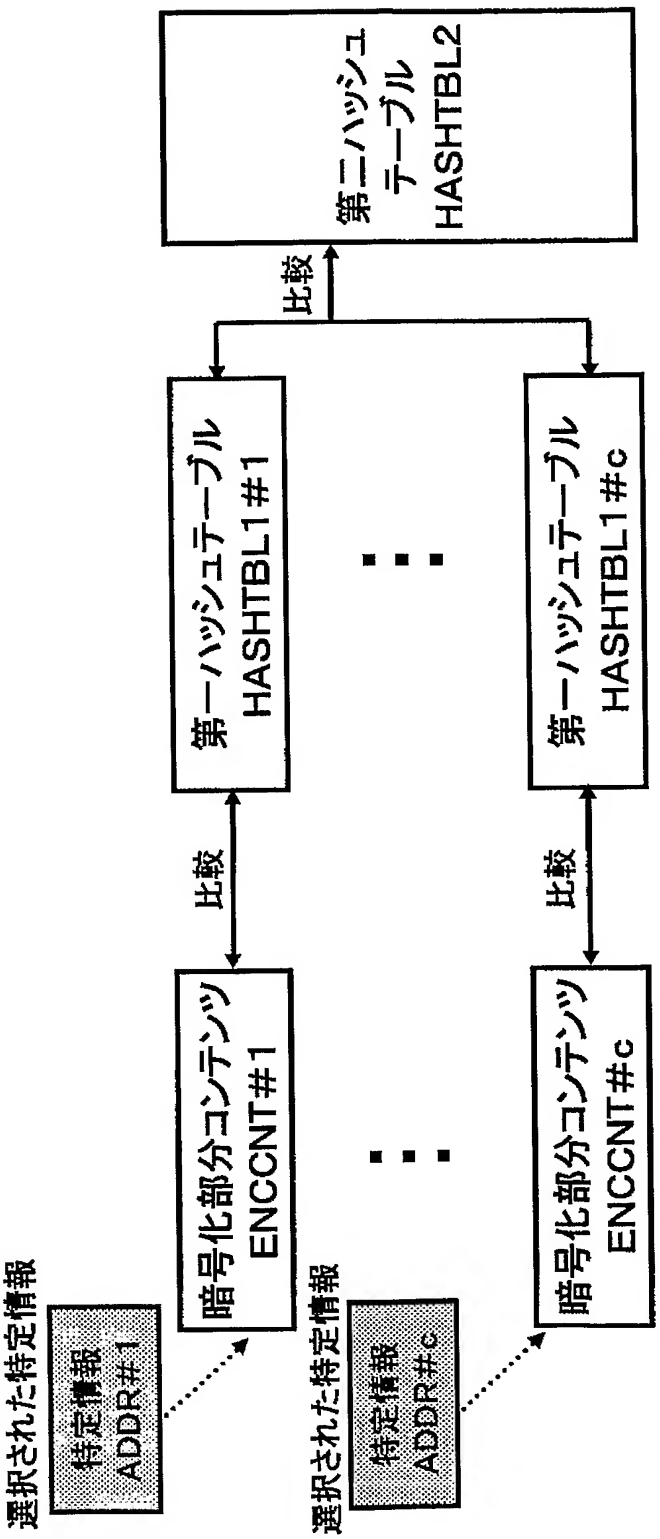
【図２４】

認証情報AUTHの別の検証例（ステップ1）

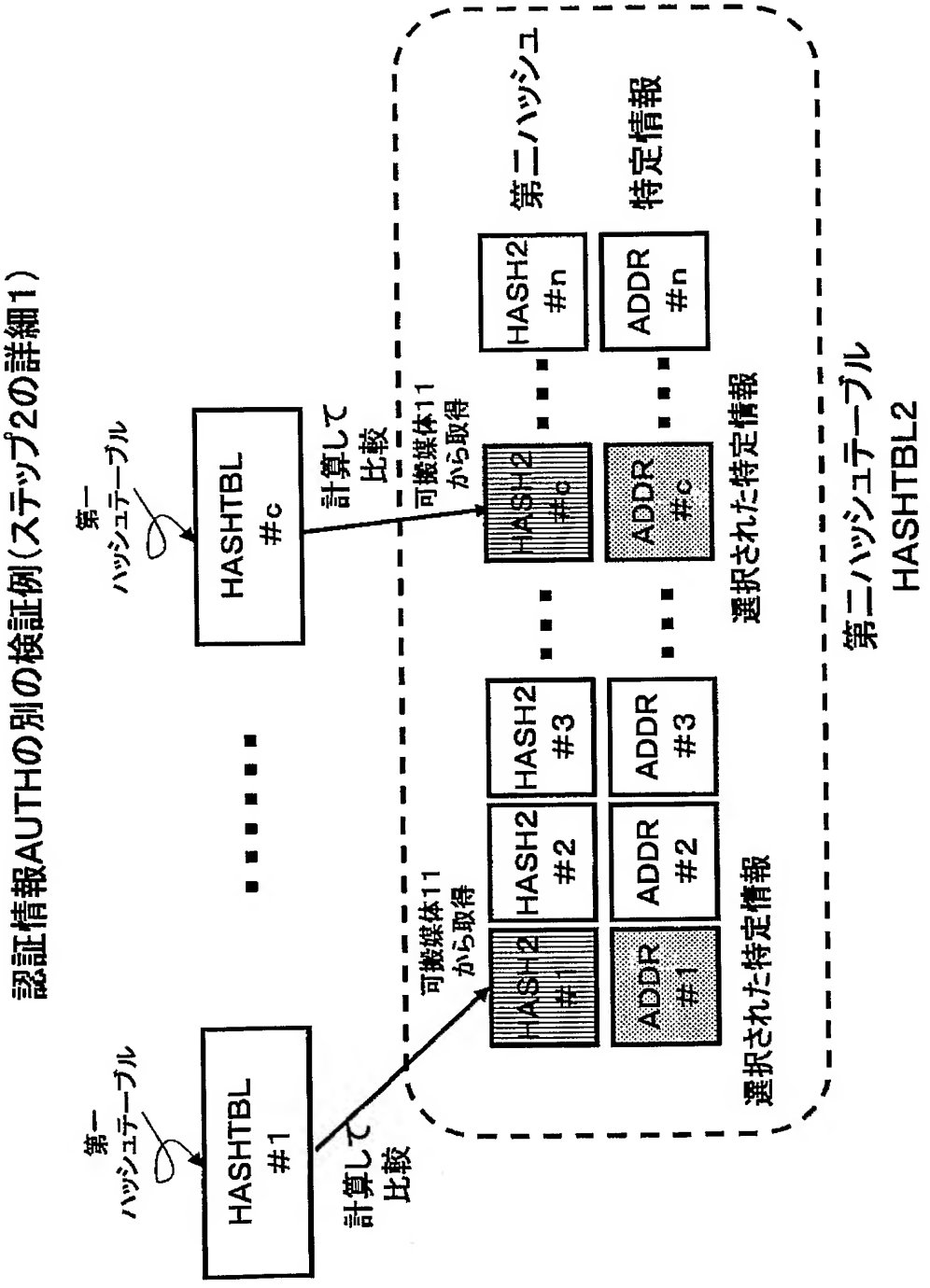


【図２５】

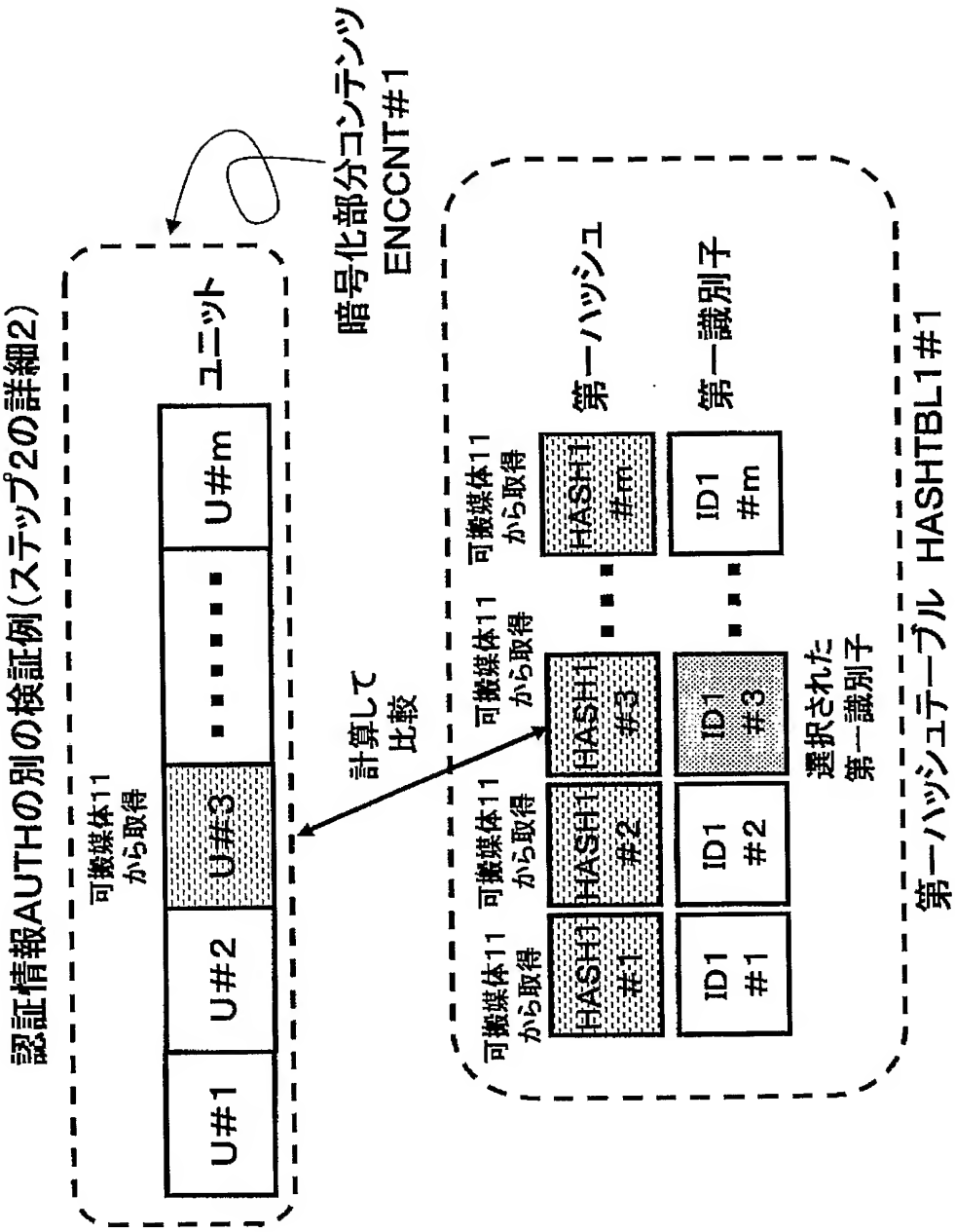
認証情報AUTHの別の検証例(ステップ2)



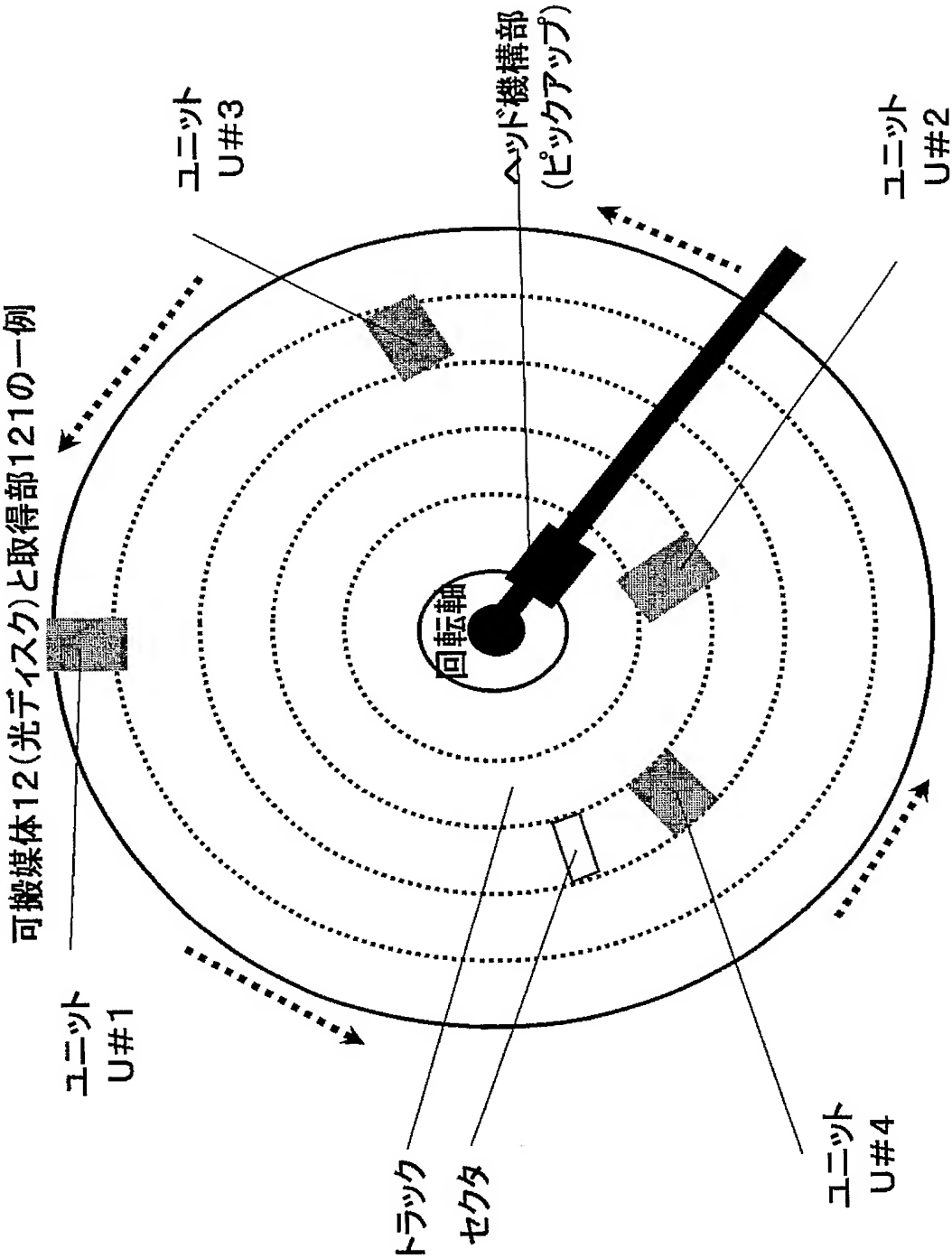
【図２６】


認証情報AUTHの別の検証例(ステップ2の詳細1)
第一ハッシュテーブル
HASHTBL #1
HASHTBL #c
計算して比較
可搬媒体11から取得
HASH2 #1
HASH2 #2
HASH2 #3
HASH2 #c
HASH2 #n
第二ハッシュ
ADDR #1
ADDR #2
ADDR #3
ADDR #c
ADDR #n
特定情報
選択された特定情報
第二ハッシュテーブル
HASHTBL2

【図２７】

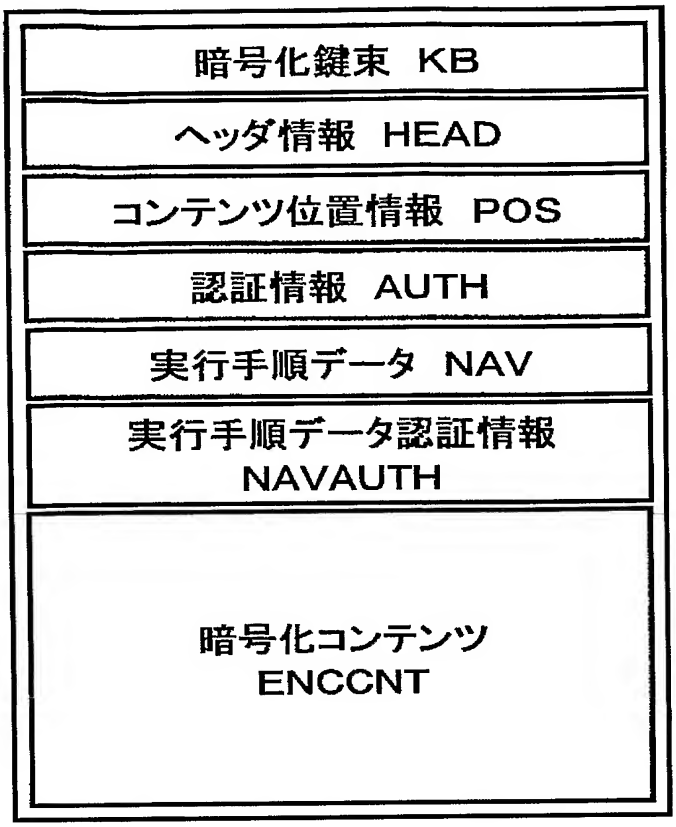

認証情報AUTHの別の検証例(ステップ2の詳細2)
暗号化部分コンテンツ
ENCCNT#1
ユニット
U#1
U#2
U#3
U#m
可搬媒体11
から取得
計算して
比較
選択された
第一識別子
第一ハッシュ
第一識別子
HASH1
#1
HASH1
#2
HASH1
#3
HASH1
#m
ID1
#1
ID1
#2
ID1
#3
ID1
#m
第一ハッシュテーブル HASHTBL1#1

【図２８】


ユニット
U#3
ヘッド機構部
(ピックアップ)
ユニット
U#2
可搬媒体12(光ディスク)と取得部121の一例
回転軸
ユニット
U#1
トラック
セクタ
ユニット
U#4

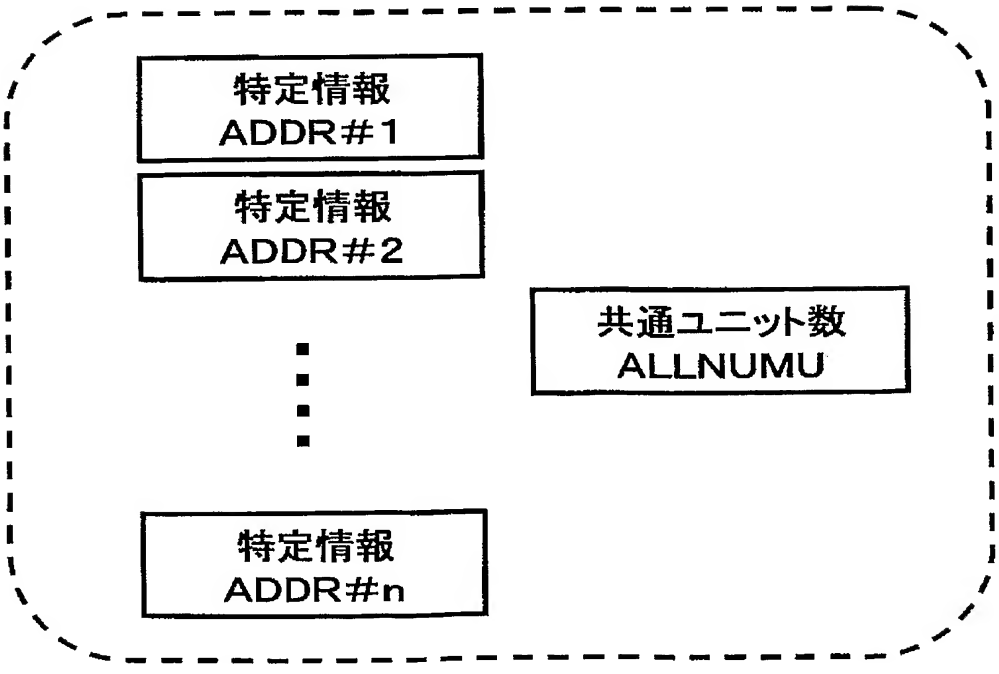
【図２９】

可搬媒体１１に記録されるデータの別の一例



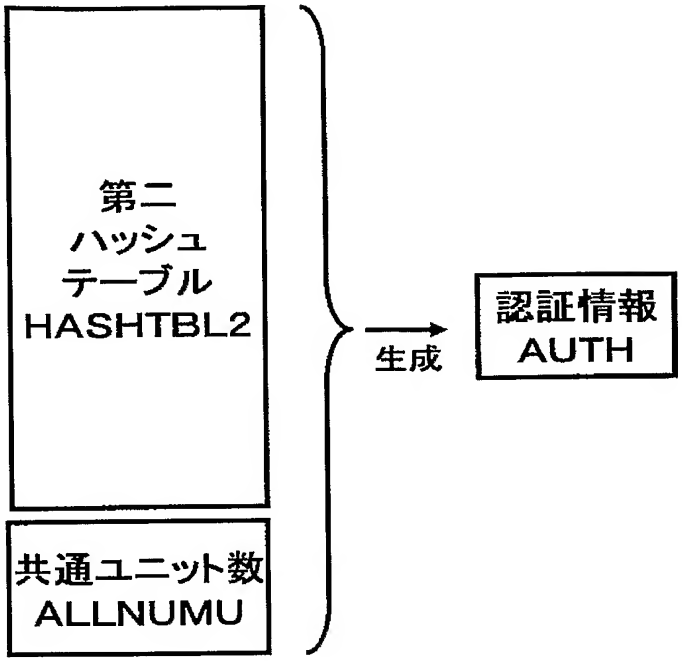
【図３０】

コンテンツ位置情報　POSの別の一例



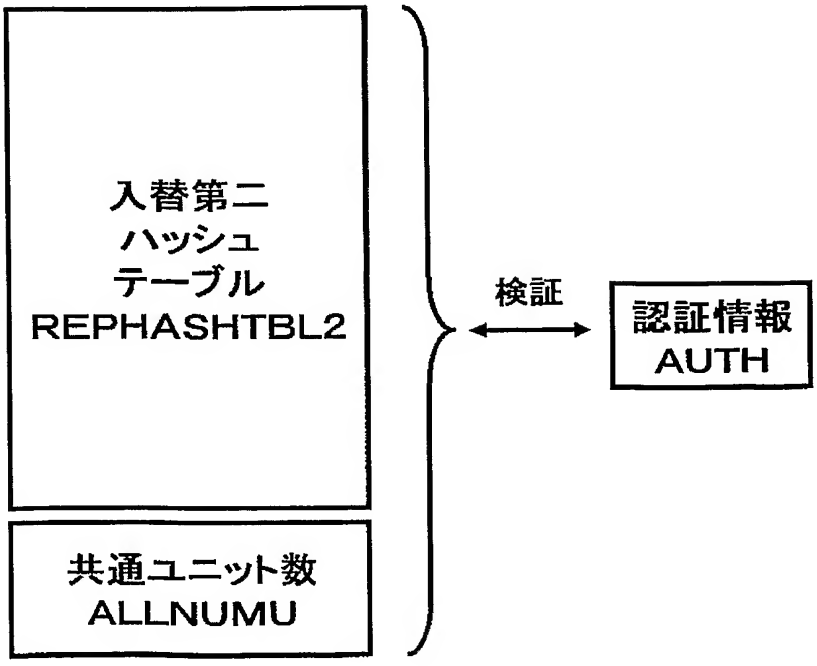
【図３１】

認証情報AUTHの作成方法の別の一例



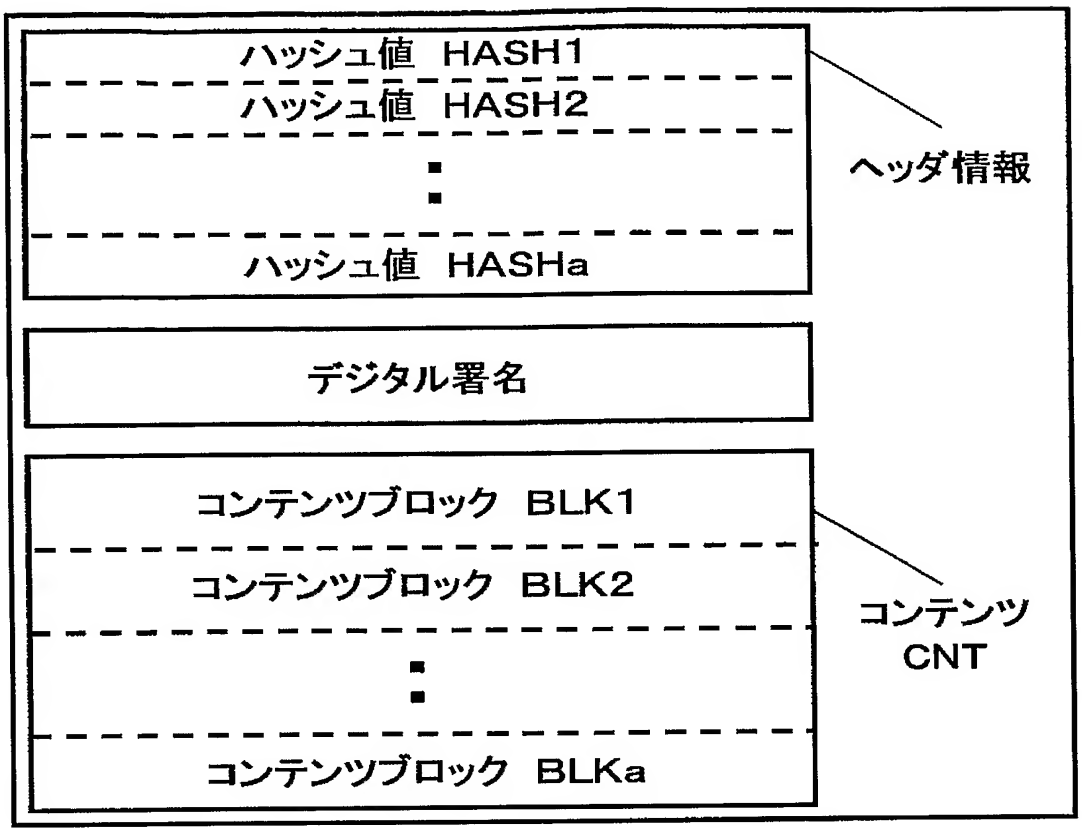
【図３２】

認証情報AUTHの検証方法の別の一例



【図３３】

従来技術の可搬媒体に記録されるデータ



【書類名】要約書
【要約】
【課題】実行装置において不正コンテンツかどうか検知する処理において、コンテンツ実行中の処理負荷が大きかった。
【解決手段】配布センタ１０が、暗号化されたコンテンツＣＮＴとともに、ヘッダ情報ＨＥＡＤ、及び、コンテンツ位置情報ＰＯＳ、及び、認証情報ＡＵＴＨ（例えばデジタル署名）を可搬媒体１１に記録し、実行装置１２では、コンテンツＣＮＴの実行、再生開始前に、認証情報ＡＵＴＨが正規の認証情報（例えばデジタル署名）であるか検証する際に、コンテンツ位置情報ＰＯＳに含まれるｎ組の特定情報ＡＤＤＲ＃１、・・・、ＡＤＤＲ＃ｎとユニット数Ｕ＃１、・・・、Ｕ＃ｎから、ｉ組の特定情報とユニット数を選択し、一部のハッシュ値に絞って検証することにより、コンテンツＣＮＴを実行、再生開始する毎に、異なるハッシュ値を選択する。
【選択図】図１

特願２００４－１９６５３１

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社